P-660R-T1 v3

ADSL2+ Access Router

User's Guide

Version 3.40
10/2008
Edition 1

DEFAULT LOGIN	
IP Address	**http://192.168.1.1**
User Name	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

It is recommended you use the web configurator to configure the ZyXEL Device.

- Supporting Disc
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Disclaimer

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

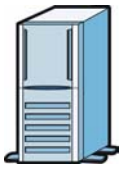
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-660R-T1 v3 may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device	Computer	Notebook computer
Server 	Firewall	Telephone
Router	Switch	

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

This product is recyclable. Dispose of it properly.

Contents Overview

Introduction **25**

Introducing the ZyXEL Device 27
Introducing the Web Configurator 31

Status **35**

Device Information 37
System Logs 39
Traffic Statistics 41

Quick Start Wizard **43**

Quick Start Wizard 45

Interface Setup **51**

Internet Setup 53
LAN Setup 67

Advanced Setup **75**

Static Route 77
Network Address Translation (NAT) 81
Quality of Service (QoS) 91
ADSL 99
Firewall 101

Access Management **103**

Access Control 105
Filters 109
SNMP 115
Universal Plug-and-Play (UPnP) 117
Dynamic DNS Setup 129
CWMP 131

Maintenance **135**

Administrator Settings 137
Time Zone 139
Firmware 141
System Restart 149
Diagnostic 151

Troubleshooting and Product Specifications 153

Troubleshooting 155
Product Specifications 159

Appendices and Index 165

Table of Contents

About This User's Guide 3

Document Conventions 4

Safety Warnings 6

Contents Overview 9

Table of Contents 11

List of Figures 19

List of Tables 23

Part I: Introduction 25

Chapter 1
Introducing the ZyXEL Device 27

1.1 Overview 27
1.2 Ways to Manage the ZyXEL Device 27
1.3 Good Habits for Managing the ZyXEL Device 28
1.4 Applications for the ZyXEL Device 28
1.4.1 Internet Access 28
1.5 LEDs (Lights) 29
1.6 The RESET Button 30
1.6.1 Using the Reset Button 30

Chapter 2
Introducing the Web Configurator 31

2.1 Overview 31
2.1.1 Accessing the Web Configurator 31
2.2 Web Configurator Main Screen 32
2.2.1 Navigation Panel 33
2.2.2 Main Window 34

Part II: Status 35

Chapter 3
Device Information 37

3.1 Overview 37
3.2 The Device Info Screen 37

Chapter 4
System Logs 39

4.1 Overview 39
4.2 The System Log Screen 39

Chapter 5
Traffic Statistics 41

5.1 Overview 41
5.2 The Statistics Screen 41

Part III: Quick Start Wizard 43

Chapter 6
Quick Start Wizard 45

6.1 Overview 45
6.2 Quick Start Wizard 45

Part IV: Interface Setup 51

Chapter 7
Internet Setup 53

7.1 Overview 53
7.1.1 What You Can Do in the Internet Screens 53
7.1.2 What You Need to Know About ADSL Internet Access 53
7.1.3 Before You Begin 54
7.2 The Internet Screen 55
7.2.1 Dynamic IP Address 56
7.2.2 Static IP Address 58
7.2.3 PPPoA/PPPoE 60
7.2.4 Bridge Mode 62
7.2.5 The PVCs Summary Screen 62
7.3 WAN Technical Reference 63
7.3.1 Encapsulation 63
7.3.2 Multiplexing 64

7.3.3 VPI and VCI 64
7.3.4 IP Address Assignment 64
7.3.5 Always-On Connection (PPP) 65
7.3.6 ATM QoS 65
7.3.7 ATM Traffic Classes 66

Chapter 8
LAN Setup 67

8.1 Overview 67
8.1.1 What You Can Do in the LAN Screens 67
8.1.2 What You Need To Know About LAN 67
8.2 The LAN Screen 68
8.2.1 The DHCP IP Pool Summary Screen 70
8.3 LAN Technical Reference 71
8.3.1 LANs, WANs and the ZyXEL Device 71
8.3.2 DHCP Setup 71
8.3.3 DNS Server Addresses 72
8.3.4 LAN TCP/IP 72
8.3.5 RIP Setup 73
8.3.6 Multicast 74

Part V: Advanced Setup 75

Chapter 9
Static Route 77

9.1 Overview 77
9.1.1 What You Can Do in the Static Route Screens 77
9.2 The Routing Table List Screen 78
9.2.1 The Static Route Screen 78

Chapter 10
Network Address Translation (NAT) 81

10.1 Overview 81
10.1.1 What You Can Do in the NAT Screens 81
10.1.2 What You Need To Know About NAT 81
10.2 The NAT Screen 82
10.3 The DMZ Screen 83
10.4 The Virtual Server Screen 84
10.4.1 Configuring Servers Behind Port Forwarding (Example) 84
10.4.2 Configuring the Virtual Server Screen 85
10.5 The IP Address Mapping Screen 86

10.6 NAT Technical Reference 88
10.6.1 NAT Definitions 88
10.6.2 What NAT Does 89
10.6.3 How NAT Works 89

Chapter 11
Quality of Service (QoS) 91

11.1 Overview 91
11.1.1 What You Can Do in the QoS Screens 92
11.1.2 What You Need to Know About QoS 92
11.2 The QoS Screen 93
11.2.1 The QoS Settings Summary Screen 95
11.3 QoS Technical Reference 96
11.3.1 IEEE 802.1p 96
11.3.2 IP Precedence 96
11.3.3 Automatic Priority Queue Assignment 97

Chapter 12
ADSL 99

12.1 Overview 99
12.2 The ADSL Screen 99

Chapter 13
Firewall 101

13.1 Overview 101
13.1.1 What You Can Do in the Firewall Screens 101
13.1.2 What You Need to Know About Firewall 101
13.2 The Firewall Screen 102

Part VI: Access Management 103

Chapter 14
Access Control 105

14.1 Access Control Overview 105
14.1.1 The Access Control Setup Screen 105
14.1.2 Access Control Interfaces 105
14.1.3 System Timeout 106
14.1.4 Configuring the Access Control Setup Screen 106

Chapter 15
Filters 109

15.1 Overview 109
15.1.1 What You Can Do in the Filter Screens 109
15.1.2 What You Need to Know About Filtering 109
15.2 The IP/MAC Filter Screen 110
15.3 The Application Filter Screen 112
15.4 The URL Filter Screen 113

Chapter 16
SNMP 115

16.1 Overview 115
16.1.1 Supported MIBs 116
16.2 The SNMP Screen 116

Chapter 17
Universal Plug-and-Play (UPnP) 117

17.1 Overview 117
17.1.1 What You Can Do in the UPnP Screen 117
17.1.2 What You Need to Know About UPnP 117
17.2 The UPnP Screen 118
17.3 Installing UPnP in Windows Example 119
17.4 Using UPnP in Windows XP Example 122

Chapter 18
Dynamic DNS Setup 129

18.1 Overview 129
18.1.1 What You Can Do in the DDNS Screen 129
18.1.2 What You Need To Know About DDNS 129
18.2 The Dynamic DNS Screen 130

Chapter 19
CWMP 131

19.1 Overview 131
19.2 The CWMP Setup Screen 132

Part VII: Maintenance 135

Chapter 20
Administrator Settings 137

20.1 Overview 137
20.2 The Administrator Screen 137

Chapter 21
Time Zone 139

21.1 Overview 139
21.2 The Time Zone Screen 139

Chapter 22
Firmware 141

22.1 Overview 141
22.1.1 What You Need To Know About Firmware 141
22.1.2 Before You Begin 142
22.1.3 Firmware and Configuration Files Examples 142
22.2 The Firmware Screen 146

Chapter 23
System Restart 149

23.1 Overview 149
23.2 The System Restart Screen 149

Chapter 24
Diagnostic 151

24.1 Overview 151
24.2 The Diagnostic Screen 151

Part VIII: Troubleshooting and Product Specifications 153

Chapter 25
Troubleshooting 155

25.1 Power, Hardware Connections, and LEDs 155
25.2 ZyXEL Device Access and Login 156
25.3 Internet Access 157

Chapter 26
Product Specifications 159

26.1 Hardware Specifications 159
26.2 Firmware Specifications 159
26.3 Power Adaptor Specifications 162

Part IX: Appendices and Index 165

Appendix A Setting up Your Computer's IP Address 167

Appendix B Pop-up Windows, JavaScripts and Java Permissions 189

Appendix C IP Addresses and Subnetting 197

Appendix D Services 205

Appendix E Legal Information 209

Appendix F Customer Support 213

Index 219

List of Figures

Figure 1 ZyXEL Device's Router Features 28
Figure 2 LEDs on the Top of the Device 29
Figure 3 Login Screen 32
Figure 4 Main Screen 32
Figure 5 Status > Device Information 37
Figure 6 Status > System Log 39
Figure 7 Status > Statistics (Ethernet) 41
Figure 8 Status > Statistics (ADSL) 42
Figure 9 Access Quick Start Wizard 45
Figure 10 Run Wizard 46
Figure 11 Wizard Summary 46
Figure 12 Password 46
Figure 13 Time Zone 47
Figure 14 ISP Connection Type 47
Figure 15 ISP Connection: Dynamic IP 47
Figure 16 ISP Connection: Static IP Address 48
Figure 17 ISP Connection: PPPoE/PPPoA 49
Figure 18 ISP Connection: Bridge Mode 49
Figure 19 Complete Quick Start 50
Figure 20 LAN and WAN 53
Figure 21 Interface Setup > Internet 55
Figure 22 Interface Setup > Internet (Dynamic IP) 56
Figure 23 Interface Setup > Internet (Static IP) 58
Figure 24 Interface Setup > Internet (PPPoA/PPPoE) 60
Figure 25 Interface Setup > Internet (Bridge) 62
Figure 26 Interface Setup > PVCs Summary 62
Figure 27 Example of ATM QoS 65
Figure 28 Interface Setup > LAN 69
Figure 29 Interface Setup > LAN > DHCP IP Pool Summary 70
Figure 30 LAN and WAN IP Addresses 71
Figure 31 Example of Static Routing Topology 77
Figure 32 Advanced Setup > Routing Table List 78
Figure 33 Advanced > Routing > Static Route 78
Figure 34 Advanced Setup > NAT 82
Figure 35 Advanced Setup > NAT > DMZ 83
Figure 36 Multiple Servers Behind NAT Example 84
Figure 37 Advanced Setup > NAT > Virtual Server 85
Figure 38 Advanced Setup > NAT > IP Address Mapping 87

Figure 39 How NAT Works 90
Figure 40 QoS Example 91
Figure 41 Advanced Setup > QoS 93
Figure 42 Advanced Setup > QoS > QoS Settings Summary 95
Figure 43 Advanced Setup > ADSL 99
Figure 44 Advanced Setup > Firewall 102
Figure 45 Access Control 105
Figure 46 Access Management > ACL 106
Figure 47 Access Management > Filter (IP/MAC) 110
Figure 48 Access Management > Filter (Application) 112
Figure 49 Access Management > Filter (URL) 113
Figure 50 SNMP Management Model 115
Figure 51 Access Management > SNMP 116
Figure 52 Access Management > UPnP 118
Figure 53 Add/Remove Programs: Windows Setup: Communication 119
Figure 54 Add/Remove Programs: Windows Setup: Communication: Components 120
Figure 55 Network Connections 120
Figure 56 Windows Optional Networking Components Wizard 121
Figure 57 Networking Services 121
Figure 58 Network Connections 122
Figure 59 Internet Connection Properties 123
Figure 60 Internet Connection Properties: Advanced Settings 124
Figure 61 Internet Connection Properties: Advanced Settings: Add 124
Figure 62 System Tray Icon 125
Figure 63 Internet Connection Status 125
Figure 64 Network Connections 126
Figure 65 Network Connections: My Network Places 127
Figure 66 Network Connections: My Network Places: Properties: Example 127
Figure 67 Access Management > DDNS 130
Figure 68 LAN and WAN 131
Figure 69 Access Management > CWMP 132
Figure 70 Maintenance > Administraton 137
Figure 71 Maintenance > Time Zone 139
Figure 72 Restore Using FTP Session Example 143
Figure 73 FTP Session Example of Firmware File Upload 144
Figure 74 FTP Session Example 145
Figure 75 Maintenance > Firmware 146
Figure 76 Maintenance > System Restart 149
Figure 77 Maintenance > Diagnostic 151
Figure 78 WIndows 95/98/Me: Network: Configuration 168
Figure 79 Windows 95/98/Me: TCP/IP Properties: IP Address 169
Figure 80 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 170
Figure 81 Windows XP: Start Menu 171

Figure 82 Windows XP: Control Panel 171
Figure 83 Windows XP: Control Panel: Network Connections: Properties 172
Figure 84 Windows XP: Local Area Connection Properties 172
Figure 85 Windows XP: Internet Protocol (TCP/IP) Properties 173
Figure 86 Windows XP: Advanced TCP/IP Properties 174
Figure 87 Windows XP: Internet Protocol (TCP/IP) Properties 175
Figure 88 Windows Vista: Start Menu 176
Figure 89 Windows Vista: Control Panel 176
Figure 90 Windows Vista: Network And Internet 176
Figure 91 Windows Vista: Network and Sharing Center 176
Figure 92 Windows Vista: Network and Sharing Center 177
Figure 93 Windows Vista: Local Area Connection Properties 177
Figure 94 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties 178
Figure 95 Windows Vista: Advanced TCP/IP Properties 179
Figure 96 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties 180
Figure 97 Macintosh OS 8/9: Apple Menu 181
Figure 98 Macintosh OS 8/9: TCP/IP 181
Figure 99 Macintosh OS X: Apple Menu 182
Figure 100 Macintosh OS X: Network 183
Figure 101 Red Hat 9.0: KDE: Network Configuration: Devices 184
Figure 102 Red Hat 9.0: KDE: Ethernet Device: General 184
Figure 103 Red Hat 9.0: KDE: Network Configuration: DNS 185
Figure 104 Red Hat 9.0: KDE: Network Configuration: Activate 185
Figure 105 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 186
Figure 106 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 186
Figure 107 Red Hat 9.0: DNS Settings in resolv.conf 186
Figure 108 Red Hat 9.0: Restart Ethernet Card 186
Figure 109 Red Hat 9.0: Checking TCP/IP Properties 187
Figure 110 Pop-up Blocker 189
Figure 111 Internet Options: Privacy 190
Figure 112 Internet Options: Privacy 191
Figure 113 Pop-up Blocker Settings 191
Figure 114 Internet Options: Security 192
Figure 115 Security Settings - Java Scripting 193
Figure 116 Security Settings - Java 193
Figure 117 Java (Sun) 194
Figure 118 Mozilla Firefox: Tools > Options 195
Figure 119 Mozilla Firefox Content Security 195
Figure 120 Network Number and Host ID 198
Figure 121 Subnetting Example: Before Subnetting 200
Figure 122 Subnetting Example: After Subnetting 201

List of Tables

Table 1 LED Descriptions 29
Table 2 Navigation Panel Summary 33
Table 3 Status > Device Information 38
Table 4 Status > System Log 39
Table 5 Status > Statistics (Ethernet) 41
Table 6 Status > Statistics (ADSL) 42
Table 7 ISP Connection: Dynamic IP 48
Table 8 ISP Connection: Static IP Address 48
Table 9 ISP Connection: PPPoE/PPPoA 49
Table 10 ISP Connection: Bridge Mode 50
Table 11 Interface Setup > Internet 55
Table 12 Interface Setup > Internet (Dynamic IP) 57
Table 13 Interface Setup > Internet (Static IP) 58
Table 14 Interface Setup > Internet (PPPoA/PPPoE) 60
Table 15 Interface Setup > Internet (Bridge) 62
Table 16 Interface Setup > PVCs Summary 62
Table 17 Interface Setup > LAN 69
Table 18 Interface Setup > LAN > DHCP IP Pool Summary 71
Table 19 Advanced Setup > Routing Table List 78
Table 20 Advanced > Static Route: Edit 79
Table 21 Network > NAT > General 82
Table 22 Advanced Setup > NAT > DMZ 83
Table 23 Multiple Servers Behind NAT Example 84
Table 24 Advanced Setup > NAT > Virtual Server 85
Table 25 Network > NAT > Address Mapping 87
Table 26 NAT Definitions 89
Table 27 Advanced Setup > QoS 93
Table 28 Advanced Setup > QoS > QoS Settings Summary 95
Table 29 IEEE 802.1p Priority Level and Traffic Type 96
Table 30 Internal Layer2 and Layer3 QoS Mapping 97
Table 31 Advanced Setup > ADSL 99
Table 32 Advanced > Firewall 102
Table 33 Access Management > ACL 106
Table 34 Access Management > Filter (IP/MAC) 110
Table 35 Access Management > Filter (Application) 112
Table 36 Access Management > Filter (URL) 113
Table 37 Access Management > SNMP 116
Table 38 Access Management > UPnP 118

Table 39 Advanced > Dynamic DNS 130
Table 40 Access Management > CWMP 132
Table 41 Maintenance > Administraton 137
Table 42 Maintenance > Time Zone 139
Table 43 Filename Conventions 142
Table 44 General Commands for GUI-based FTP Clients 145
Table 45 Maintenance > Firmware 147
Table 46 Maintenance > System Restart 149
Table 47 Hardware Specifications 159
Table 48 Firmware Specifications 159
Table 49 Standards Supported 161
Table 50 ZyXEL Device Series Power Adaptor Specifications 162
Table 51 Subnet Masks 198
Table 52 Subnet Masks 199
Table 53 Maximum Host Numbers 199
Table 54 Alternative Subnet Mask Notation 199
Table 55 Subnet 1 201
Table 56 Subnet 2 202
Table 57 Subnet 3 202
Table 58 Subnet 4 202
Table 59 Eight Subnets 202
Table 60 24-bit Network Number Subnet Planning 203
Table 61 16-bit Network Number Subnet Planning 203
Table 62 Examples of Services 205

PART I
Introduction

Introducing the ZyXEL Device (27)
Introducing the Web Configurator (31)

1

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

The P-660R-T1 v3 is an ADSL2+ router. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access.

Models ending in "1", for example P-660R-T1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

All screens displayed in this user's guide are from the P-660R-T1 v3 model.

See the product specifications for a full list of features.

1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

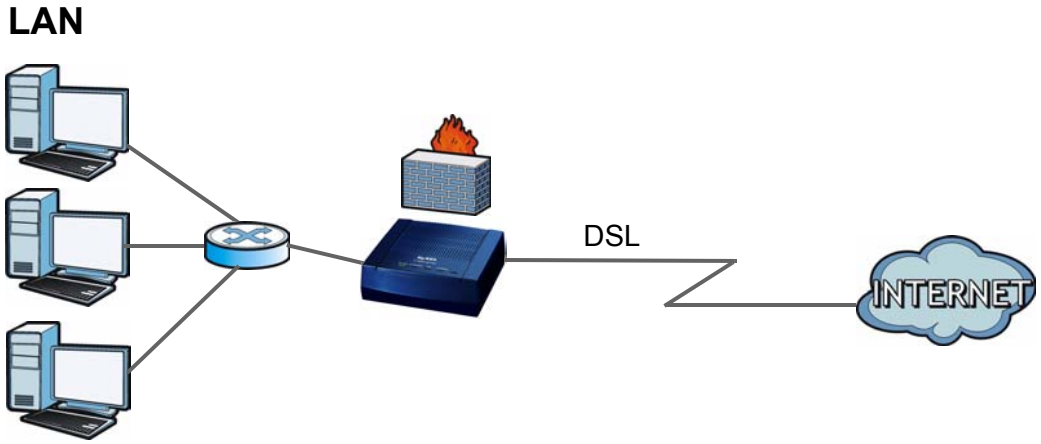
1.4 Applications for the ZyXEL Device

Here are some example uses for which the ZyXEL Device is well suited.

1.4.1 Internet Access

Your ZyXEL Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the ZyXEL Device's LAN ports.

Figure 1 ZyXEL Device's Router Features



You can also configure firewall and content filtering on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

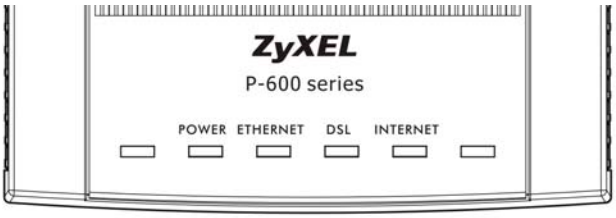
Use content filtering to block access to specific web sites, with URL's containing keywords that you specify. For example, you could block access to certain web sites for the kids.

Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the ZyXEL Device gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 2 LEDs on the Top of the Device



None of the LEDs are on if the ZyXEL Device is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and ready for use.
		Blinking	The ZyXEL Device is self-testing.
	Red	On	The ZyXEL Device detected an error while self-testing, or there is a device malfunction.
		Off	The ZyXEL Device is not receiving power.
ETHERNET	Green	On	The ZyXEL Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The ZyXEL Device is sending/receiving data to /from the LAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the LAN.
DSL	Green	On	The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The ZyXEL Device is sending or receiving IP traffic.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The ZyXEL Device does not have an IP connection.

Refer to the Quick Start Guide for information on hardware connections.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

1.6.1 Using the Reset Button

1. Make sure the **POWER** LED is on (not blinking).
2. To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

2

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

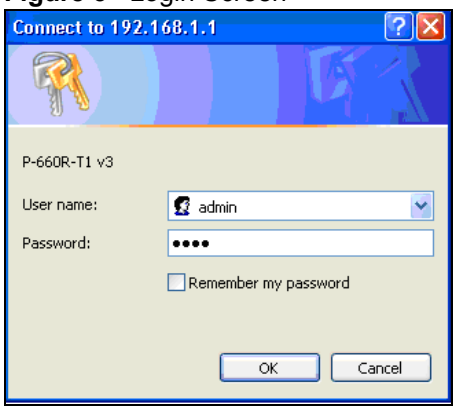
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See Appendix B on page 189 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

1. Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. A login screen displays. To access the administrative web configurator and manage the ZyXEL Device, enter the username (admin by default) and password (1234 by default) in the login screen and click **OK**. If you have changed the password, enter your password and click **OK**.

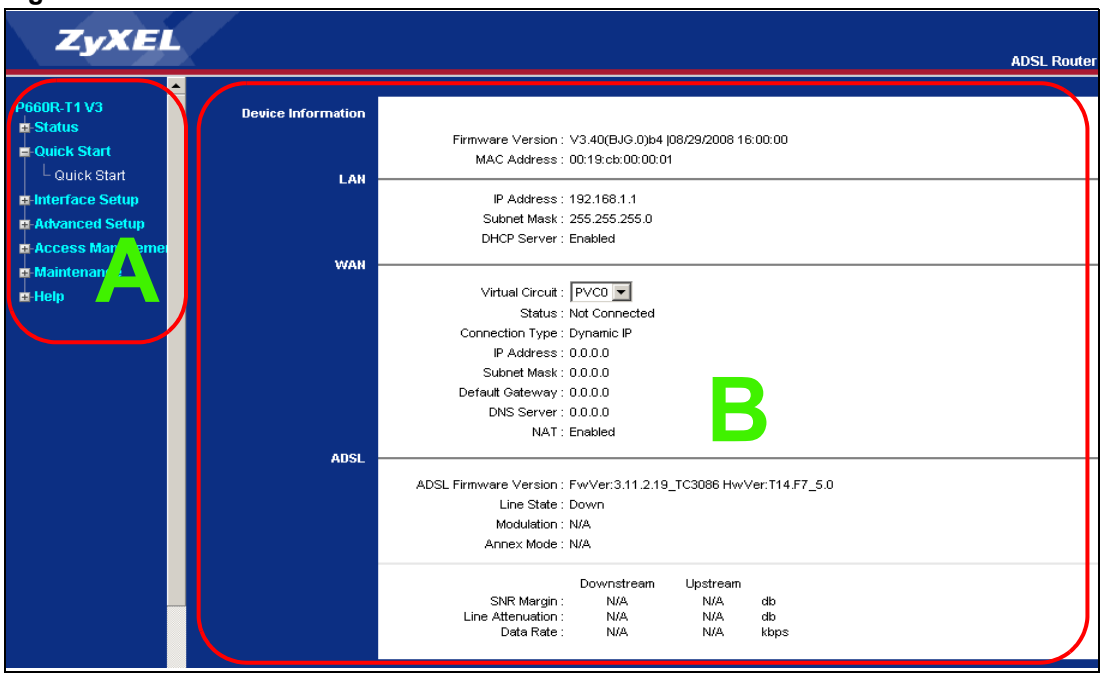
Figure 3 Login Screen



For security reasons, the ZyXEL Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

2.2 Web Configurator Main Screen

Figure 4 Main Screen



As illustrated above, the main screen is divided into these parts:

- **A** - navigation panel
- **B** - main window

2.2.1 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following tables describe each menu item.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		
Device Info		This screen shows the ZyXEL Device's general device and network status information.
System Log		Use this screen to display your device's logs.
Statistics		Use this screen to display the statistics of the ZyXEL Device.
Quick Start		
Quick Start		Use this wizard to set up your Internet connection.
Interface Setup		
Internet	Internet	Use this screen to configure ISP parameters, WAN IP address assignment and other advanced properties.
	PVC Summary Table	Use this screen to display your PVC settings.
LAN	LAN	Use this screen to configure LAN TCP/IP and DHCP settings and other advanced properties.
	DHCP IP Pool Summary	Use this screen to display the IP and MAC addresses of the computers on your LAN.
Advanced Setup		
Routing	Routing Table List	Use this screen to display the static routes on your ZyXEL Device.
	Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
NAT	NAT	Use this screen to configure the NAT settings.
	DMZ	Use this screen to configure the DMZ settings.
	Virtual Server	Use this screen to forward incoming service requests to the server(s) on your local network.
	IP Address Mapping	Use this screen to change your ZyXEL Device's address mapping settings.
QoS	QoS	Use this screen to enable QoS and traffic prioritizing and configure bandwidth management on the WAN.
	QoS Settings Summary	Use this screen to check the QoS rules and actions you configured for the ZyXEL Device.
ADSL		Use this screen to configure the ADSL settings on your ZyXEL Device.
Firewall		Use this screen to activate/deactivate the firewall and/or SPI on your ZyXEL Device.
Access Management		
ACL		Use this screen to determine which application can access which ZyXEL Device interface from which computers.
Filter	IP/MAC Filter	Use this screen to to create IP/MAC filter rules.
	Application Filter	Use this screen to set the days and times for your device to perform content filtering.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
	URL Filter	Use this screen to allow or deny traffic from certain types of applications.
SNMP		Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
UPnP		Use this screen to turn UPnP on or off.
DDNS		This screen allows you to use a static hostname alias for a dynamic IP address.
CWMP		Use this screen to have a management server manage the ZyXEL Device.
Maintenance		
Administraton		Use this screen to configure your device's password.
Time Zone		Use this screen to change your ZyXEL Device's time and date.
Firmware		Use this screen to manage configuration files and upload firmware to your device.
SysRestart		This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic		Use this screen to test the connections to other devices.

2.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 3 on page 37 for more information about the **Status** screen.

PART II
Status

Device Information (37)
System Logs (39)
Traffic Statistics (41)

3

Device Information

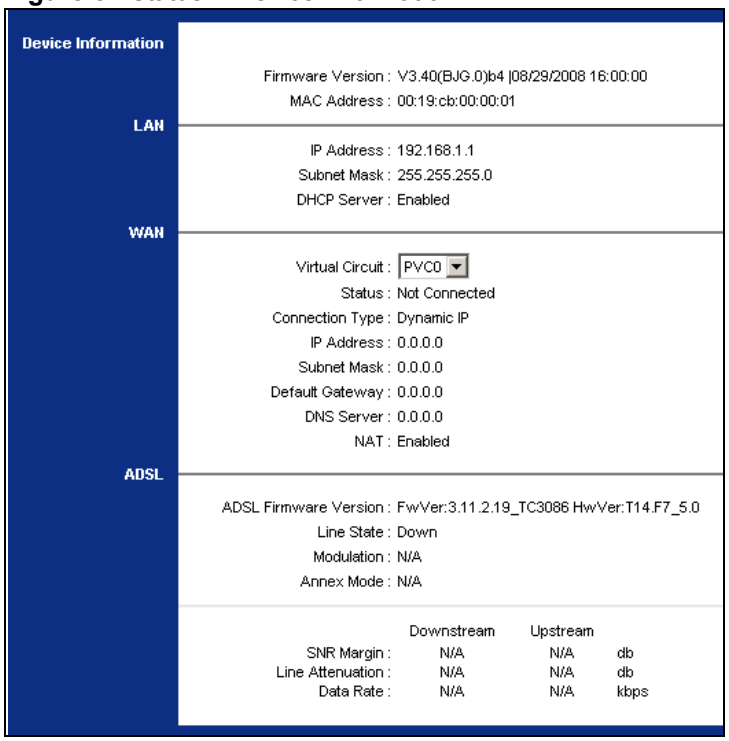
3.1 Overview

Use the **Device Info** screen to look at the current status of the device, system resources, and interfaces (LAN and WAN).

3.2 The Device Info Screen

Use this screen to view the status of the ZyXEL Device. Click **Status** > **Device Info** to open the following screen.

Figure 5 Status > Device Information



The following table describes the fields in this screen.

Table 3 Status > Device Information

LABEL	DESCRIPTION
Device Information	
Firmware Version	This is the current version of the firmware inside the device. It also shows the date the firmware version was created.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
LAN	
IP Address	This is the current IP address of the ZyXEL Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
DHCP Server	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Enabled** - The ZyXEL Device is a DHCP server in the LAN. It can assign IP addresses to other computers in the LAN. **Relay** - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **Disabled** - The ZyXEL Device is not providing any DHCP services to the LAN.
WAN	
Virtual Circuit	Use the drop-down list box to select a virtual circuit. The fields below display information about the virtual circuit you choose.
Status	This is the status of the WAN connection.
Connection Type	This is the connection type supported by your ISP.
IP Address	This is the current IP address of the ZyXEL Device in the WAN, if applicable.
IP Subnet Mask	This is the current subnet mask in the WAN, if applicable.
Default Gateway	This is the IP address of the default gateway, if applicable.
DNS Server	This is the current DNS server in the WAN, if applicable.
NAT	This field displays whether NAT is activated.
ADSL	
ADSL Firmware Version	This is the current version of the device's DSL modem code.
Line State	This is the status of your ADSL connection.
Modulation	This is the ADSL modulation of your ZyXEL Device.
Annex Mode	This is the annex mode of your ZyXEL Device.
Downstream	This is the downstream speed of your ZyXEL Device.
Upstream	This is the upstream speed of your ZyXEL Device.
SNR Margin	This is the Signal to Noise Ratio (SNR) margin. SNR represents the ratio of the signal received to the system's noise threshold. The higher the SNR number, the better the line quality.
Line Attenuation	This is the difference (in dB) between the power received at the near-end and that transmitted from the far-end.
Data Rate	This is speed of data transfer on your ZyXEL Device.

4

System Logs

4.1 Overview

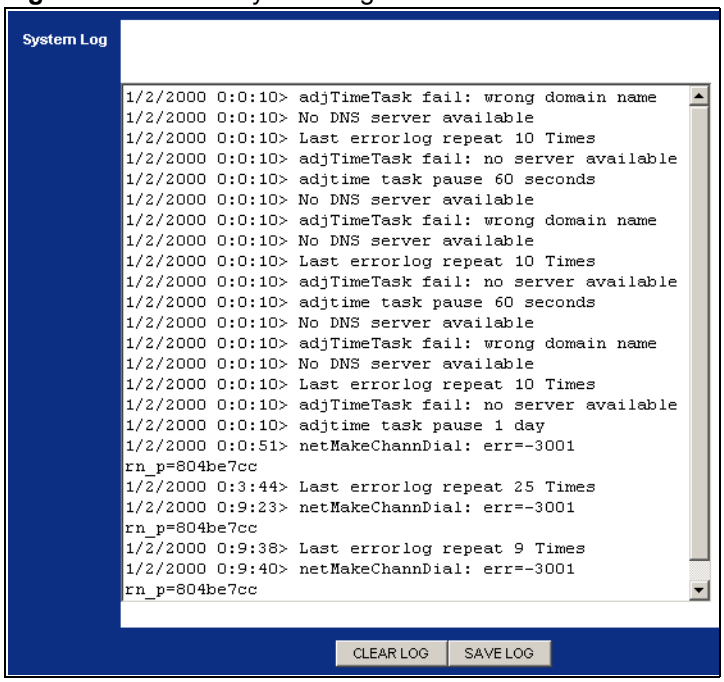
This chapter contains information about viewing the ZyXEL Device's logs.

A log is a message about an event that occurred on your ZyXEL Device. For example, when someone logs in to the ZyXEL Device.

4.2 The System Log Screen

Use this screen to see the logs for your ZyXEL Device. Click **Status > System Log** to open the following screen.

Figure 6 Status > System Log


System Log
1/2/2000 0:0:10> adjTimeTask fail: wrong domain name
1/2/2000 0:0:10> No DNS server available
1/2/2000 0:0:10> Last errorlog repeat 10 Times
1/2/2000 0:0:10> adjTimeTask fail: no server available
1/2/2000 0:0:10> adjtime task pause 60 seconds
1/2/2000 0:0:10> No DNS server available
1/2/2000 0:0:10> adjTimeTask fail: wrong domain name
1/2/2000 0:0:10> No DNS server available
1/2/2000 0:0:10> Last errorlog repeat 10 Times
1/2/2000 0:0:10> adjTimeTask fail: no server available
1/2/2000 0:0:10> adjtime task pause 60 seconds
1/2/2000 0:0:10> No DNS server available
1/2/2000 0:0:10> adjTimeTask fail: wrong domain name
1/2/2000 0:0:10> No DNS server available
1/2/2000 0:0:10> Last errorlog repeat 10 Times
1/2/2000 0:0:10> adjTimeTask fail: no server available
1/2/2000 0:0:10> adjtime task pause 1 day
1/2/2000 0:0:51> netMakeChannDial: err=-3001
rn_p=804be7cc
1/2/2000 0:3:44> Last errorlog repeat 25 Times
1/2/2000 0:9:23> netMakeChannDial: err=-3001
rn_p=804be7cc
1/2/2000 0:9:38> Last errorlog repeat 9 Times
1/2/2000 0:9:40> netMakeChannDial: err=-3001
rn_p=804be7cc
CLEAR LOG
SAVE LOG

The following table describes the fields in this screen.

Table 4 Status > System Log

LABEL	DESCRIPTION
System Log	This field displays the log messages of your ZyXEL Device.

Table 4 Status > System Log

LABEL	DESCRIPTION
CLEAR LOG	Click this to delete all the logs.
SAVE LOG	Click this to save the logs in a text file.

5

Traffic Statistics

5.1 Overview

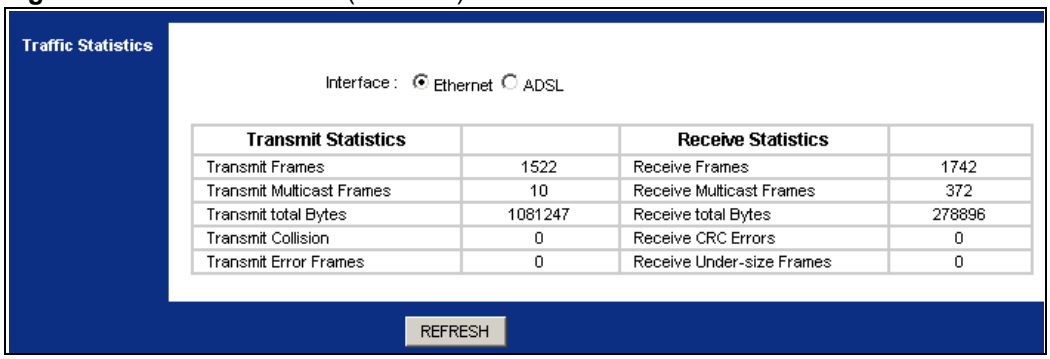
This chapter contains information about viewing traffic statistics of your ZyXEL Device.

5.2 The Statistics Screen

Use this screen to check the traffic statistics of your ZyXEL Device. Click **Status > Statistics** to open the following screen. The screen varies depending on what type of port you selected in the **Interface** field.

The following screen displays traffic statistics for the Ethernet port.

Figure 7 Status > Statistics (Ethernet)



The following table describes the labels in this screen.

Table 5 Status > Statistics (Ethernet)

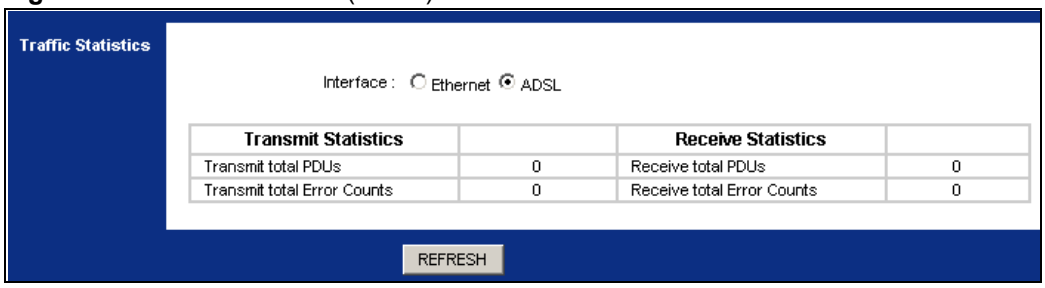
LABEL	DESCRIPTION
Interface	Select **Ethernet** or **ADSL** to display traffic statistics on the port.
Transmit Statistics	
Transmit Frames	This field displays the number of transmitted frames on this port.
Transmit Multicast Frames	This field displays the number of good multicast frames transmitted.
Transmit total Bytes	This field displays the number of bytes transmitted on this port.
Transmit Collision	This field displays information on collisions while transmitting frames.
Transmit Error Frames	This field displays the number of transmitted errors on this port.
Receive Statistics	
Receive Frames	This field displays the number of received frames on this port.

Table 5 Status > Statistics (Ethernet) (continued)

LABEL	DESCRIPTION
Receive Multicast Frames	This field displays the number of good multicast frames received.
Receive total Bytes	This field displays the number of bytes received on this port.
Receive CRC errors	This field displays the number of frames received with Cyclic Redundant Check (CRC) errors.
Receive Under-size Frames	This field displays the number of received frames that were under-size (shorter than 60 octets or greater than 1522 octets).
REFRESH	Click this to update the screen.

The following screen displays traffic statitstics for the ADSL port.

Figure 8 Status > Statistics (ADSL)



The following table describes the labels in this screen.

Table 6 Status > Statistics (ADSL)

LABEL	DESCRIPTION
Transmit Statistics	
Transmit total PDUs	This field displays the amount of Protocol Data Units (PDUs) transmitted on this port.
Transmit total Error Counts	This field displays the number of error counts transmitted on this port.
Receive Statistics	
Receive total PDUs	This field displays the amount of PDUs received on this port.
Receive total Error Counts	This field displays the number of error counts received on this port.
REFRESH	Click this to update the screen.

PART III
Quick Start Wizard

Quick Start Wizard (45)

6

Quick Start Wizard

6.1 Overview

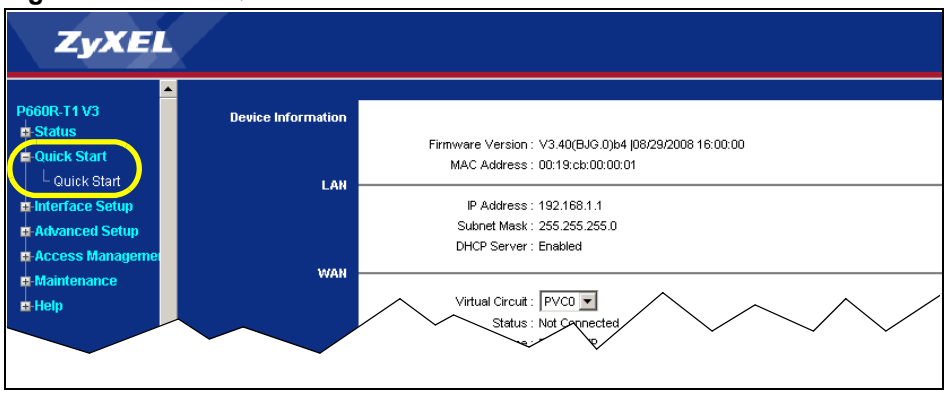
This chapter provides information on the Quick Start Wizard screens. Use the wizard screens to configure your system for Internet access with the information given to you by your ISP.

See the advanced menu chapters for background information on these fields.

6.2 Quick Start Wizard

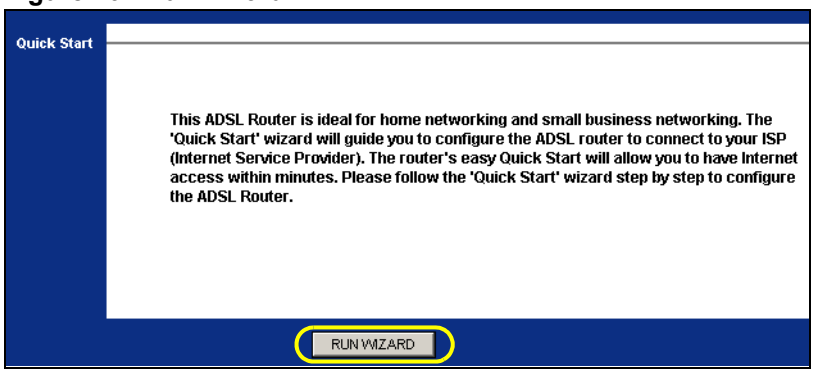
1 After you enter the password to access the web configurator, click **Quick Start** > **Quick Start** from the navigation panel to go to the wizard screens.

Figure 9 Access Quick Start Wizard



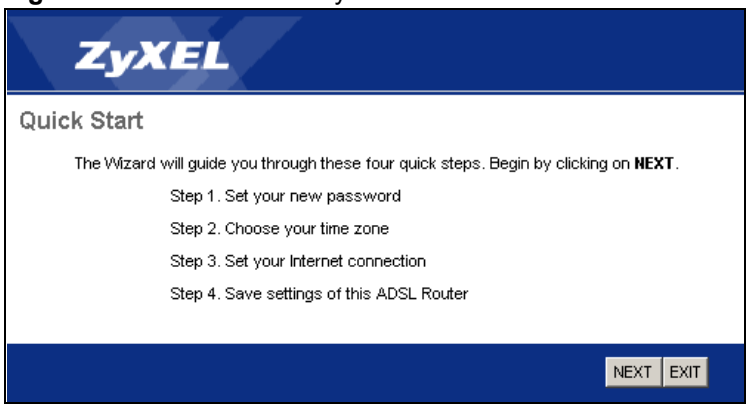
2 Click **RUN WIZARD** to configure the system for Internet access.

Figure 10 Run Wizard


Quick Start
This ADSL Router is ideal for home networking and small business networking. The 'Quick Start' wizard will guide you to configure the ADSL router to connect to your ISP (Internet Service Provider). The router's easy Quick Start will allow you to have Internet access within minutes. Please follow the 'Quick Start' wizard step by step to configure the ADSL Router.
RUN WIZARD

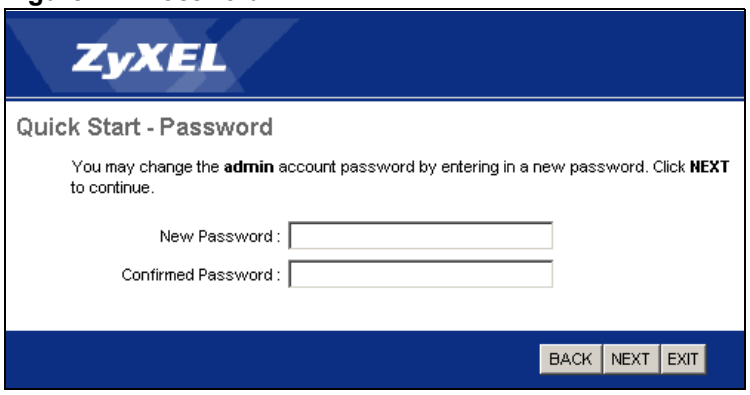
3 The following screen summarizes the steps required to configure an Internet connection. Click **NEXT** to begin the setup.

Figure 11 Wizard Summary


ZyXEL
Quick Start
The Wizard will guide you through these four quick steps. Begin by clicking on NEXT.
Step 1. Set your new password
Step 2. Choose your time zone
Step 3. Set your Internet connection
Step 4. Save settings of this ADSL Router
NEXT
EXIT

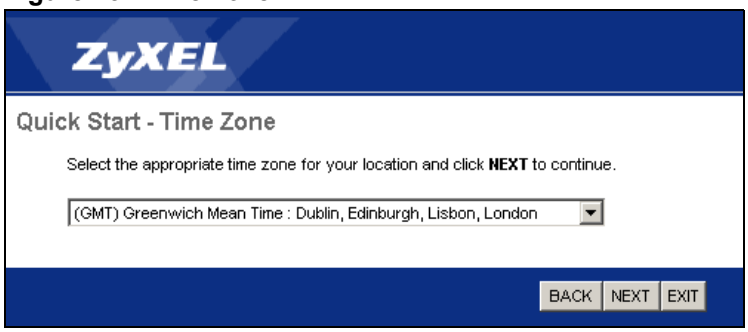
4 Enter a new password for accessing the web configurator or enter your old one if you don't want to change it. Type the new or old password in both fields and click **NEXT**.

Figure 12 Password



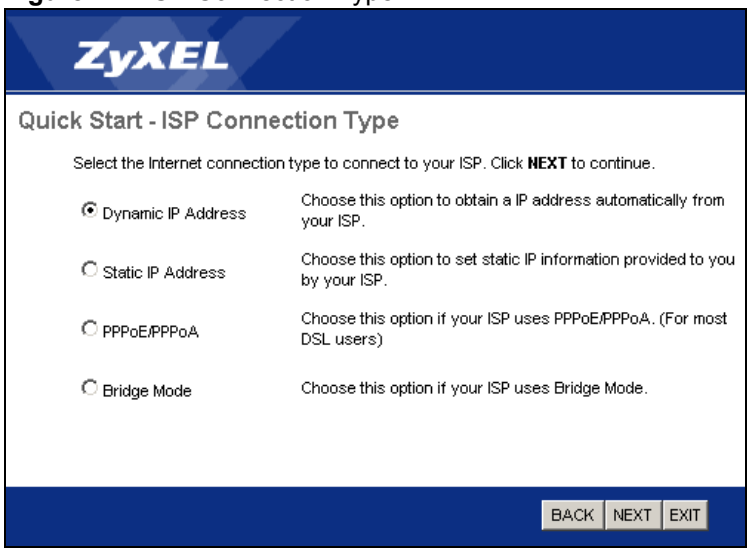
5 Select the time zone for your location and click **NEXT**.

Figure 13 Time Zone


ZyXEL
Quick Start - Time Zone
Select the appropriate time zone for your location and click NEXT to continue.
(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
BACK
NEXT
EXIT

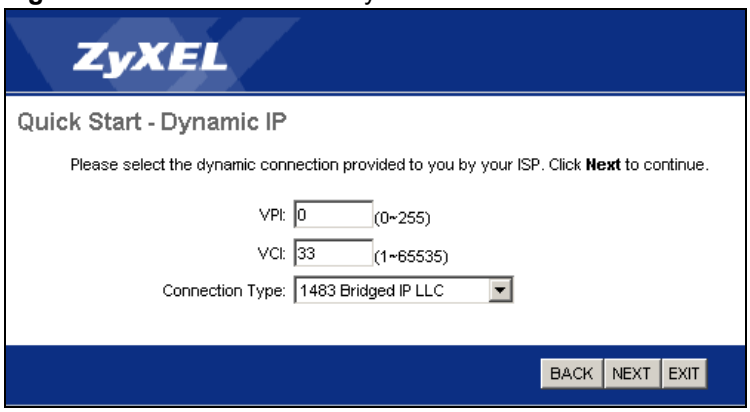
6 Select the connection type supported by your ISP and click **NEXT**.

Figure 14 ISP Connection Type


ZyXEL
Quick Start - ISP Connection Type
Select the Internet connection type to connect to your ISP. Click NEXT to continue.
Dynamic IP Address
Choose this option to obtain a IP address automatically from your ISP.
Static IP Address
Choose this option to set static IP information provided to you by your ISP.
PPPoE/PPPoA
Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)
Bridge Mode
Choose this option if your ISP uses Bridge Mode.
BACK
NEXT
EXIT

7 The next wizard screen varies depending on what connection type you use. Configure the fields and click **NEXT** to continue.

Figure 15 ISP Connection: Dynamic IP

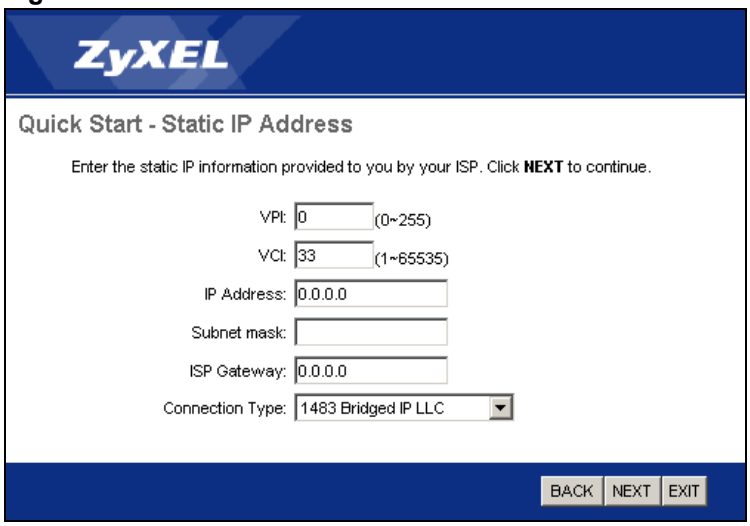

ZyXEL
Quick Start - Dynamic IP
Please select the dynamic connection provided to you by your ISP. Click Next to continue.
VPI: 0 (0~255)
VCI: 33 (1~65535)
Connection Type: 1483 Bridged IP LLC
BACK
NEXT
EXIT

The following table describes the fields in this screen.

Table 7 ISP Connection: Dynamic IP

LABEL	DESCRIPTION
VPI	Enter the VPI (Virtual Path Identifier) assigned to you. This field may already be configured. VPI defines a virtual circuit. Refer to the appendix for more information.
VCI	Enter the VCI (Virtual Channel Identifier) assigned to you. This field may already be configured. VCI defines a virtual circuit. Refer to the appendix for more information.
Connection Type	Select the multiplexing method used by your ISP from the drop-down list box. Available options are: **1483 Bridged IP LLC**, **1483 Bridged IP VC-Mux**, **1483 Routed IP LLC(IPoA)** and **1483 Routed IP VC-Mux**.
BACK	Click this to return to the previous screen without saving.
NEXT	Click this to continue to the next wizard screen.
EXIT	Click this to close the wizard screen without saving.

Figure 16 ISP Connection: Static IP Address

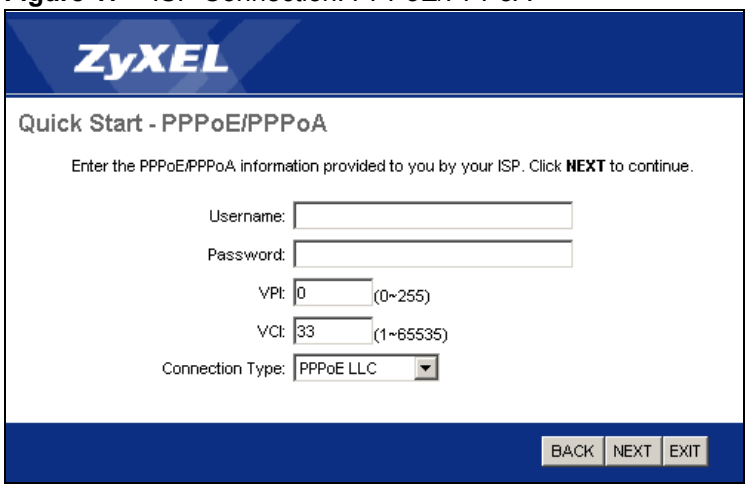


The following table describes the fields in this screen.

Table 8 ISP Connection: Static IP Address

LABEL	DESCRIPTION
VPI	Enter the VPI assigned to you. This field may already be configured. VPI defines a virtual circuit. Refer to the appendix for more information.
VCI	Enter the VCI assigned to you. This field may already be configured. VCI defines a virtual circuit. Refer to the appendix for more information.
IP Address	Type your ISP assigned IP address in this field.
Subnet mask	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask If you are implementing subnetting.
ISP Gateway	Specify a gateway IP address supplied by your ISP.
Connection Type	Select the multiplexing method used by your ISP from the drop-down list box. Available options are: **1483 Bridged IP LLC**, **1483 Bridged IP VC-Mux**, **1483 Routed IP LLC(IPoA)** and **1483 Routed IP VC-Mux**.
BACK	Click this to return to the previous screen without saving.
NEXT	Click this to continue to the next wizard screen.
EXIT	Click this to close the wizard screen without saving.

Figure 17 ISP Connection: PPPoE/PPPoA

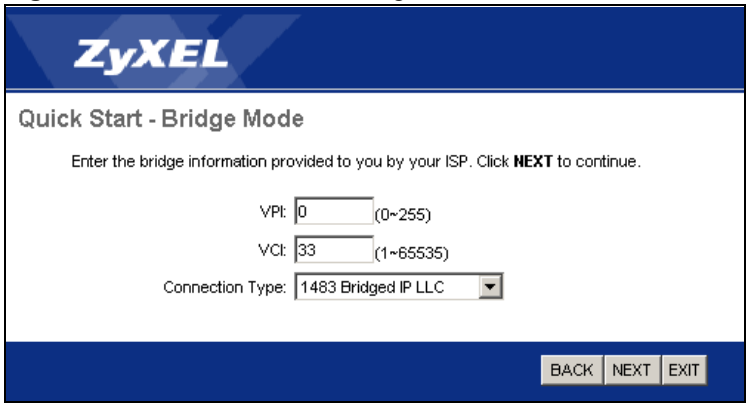


The following table describes the fields in this screen.

Table 9 ISP Connection: PPPoE/PPPoA

LABEL	DESCRIPTION
Username	Enter the username exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the above username.
VPI	Enter the VPI assigned to you. This field may already be configured. VPI defines a virtual circuit. Refer to the appendix for more information.
VCI	Enter the VCI assigned to you. This field may already be configured. VCI defines a virtual circuit. Refer to the appendix for more information.
Connection Type	Select the multiplexing method used by your ISP from the drop-down list box. Available options are: **PPPoE LLC**, **PPPoE VC-Mux**, **PPPoA LLC** and **PPPoA VC-Mux**.
BACK	Click this to return to the previous screen without saving.
NEXT	Click this to continue to the next wizard screen.
EXIT	Click this to close the wizard screen without saving.

Figure 18 ISP Connection: Bridge Mode



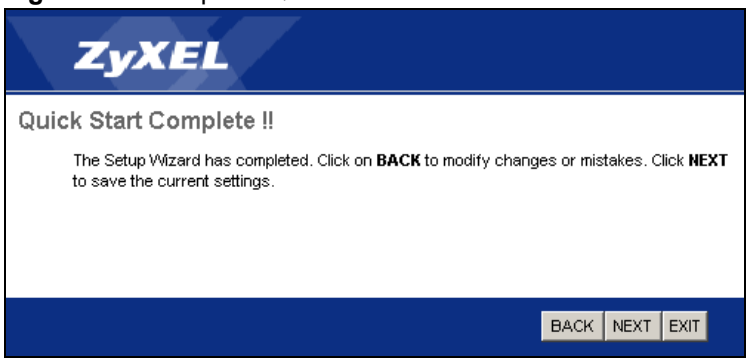
The following table describes the fields in this screen.

Table 10 ISP Connection: Bridge Mode

LABEL	DESCRIPTION
VPI	Enter the VPI assigned to you. This field may already be configured. VPI defines a virtual circuit. Refer to the appendix for more information.
VCI	Enter the VCI assigned to you. This field may already be configured. VCI defines a virtual circuit. Refer to the appendix for more information.
Connection Type	Select the multiplexing method used by your ISP from the drop-down list box. Available options are: **1483 Bridged IP LLC** and **1483 Bridged IP VC-Mux**.
BACK	Click this to return to the previous screen without saving.
NEXT	Click this to continue to the next wizard screen.
EXIT	Click this to close the wizard screen without saving.

8 Click **NEXT** to save your changes and complete the setup.

Figure 19 Complete Quick Start


ZyXEL
Quick Start Complete !!
The Setup Wizard has completed. Click on BACK to modify changes or mistakes. Click NEXT to save the current settings.
BACK
NEXT
EXIT

9 Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

PART IV
Interface Setup

Internet Setup (53)
LAN Setup (67)

7

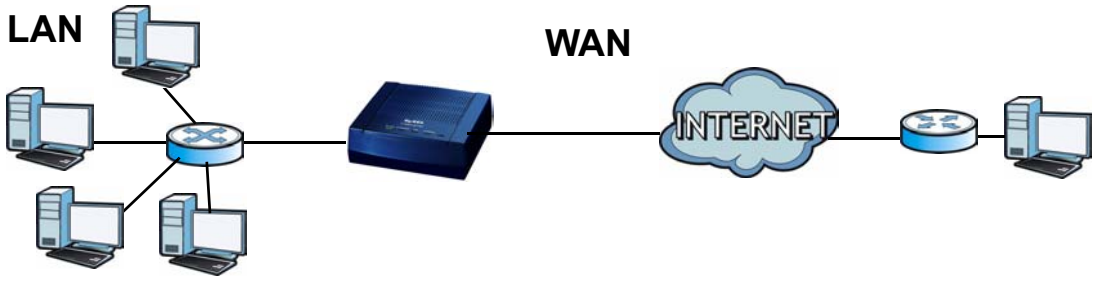
Internet Setup

7.1 Overview

This chapter describes how to configure Wide Area Network (WAN) settings from the **Internet** screens. Use these screens to configure your ZyXEL Device for Internet access.

A WAN connection is an outside connection to another network or the Internet. It connects your private networks (such as a Local Area Network (LAN) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 20 LAN and WAN



7.1.1 What You Can Do in the Internet Screens

- Use the **Internet** screen (Section 7.2 on page 55) to configure the WAN settings on the ZyXEL Device for Internet access.
- Use the **PVCs Summary** screen (Section 7.2.5 on page 62) to display a summary table for PVC settings.

7.1.2 What You Need to Know About ADSL Internet Access

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your Internet Service Provider (ISP). If your ISP offers a dial-up Internet connection using PPP over Ethernet (PPPoE) or PPPoA, they should also provide a username and password (and service name) for user authentication.

ADSL Terms

A Permanent Virtual Circuit (PVC) is the connection for your device to the ISP. You need a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI) to identify a PVC. Multiplexing is a way of carrying protocols on a PVC. Your ISP should supply you with all this information.

WAN IP Address

The WAN IP address is an IP address for the ZyXEL Device, which makes it accessible from an outside network. It is used by the ZyXEL Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the ZyXEL Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

ATM QoS

Asynchronous Transfer Mode (ATM) is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. QoS is a service agreement that guarantees certain speed even when the network is congested. ATM QoS is defined by the Peak Cell Rate (PCR), Sustain Cell Rate (SCR) and Maximum Burst Size (MBS).

NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just one.

IGMP

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 is an improvement over version 1, but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network.

Finding Out More

See Section 7.3 on page 63 for technical background information on WAN.

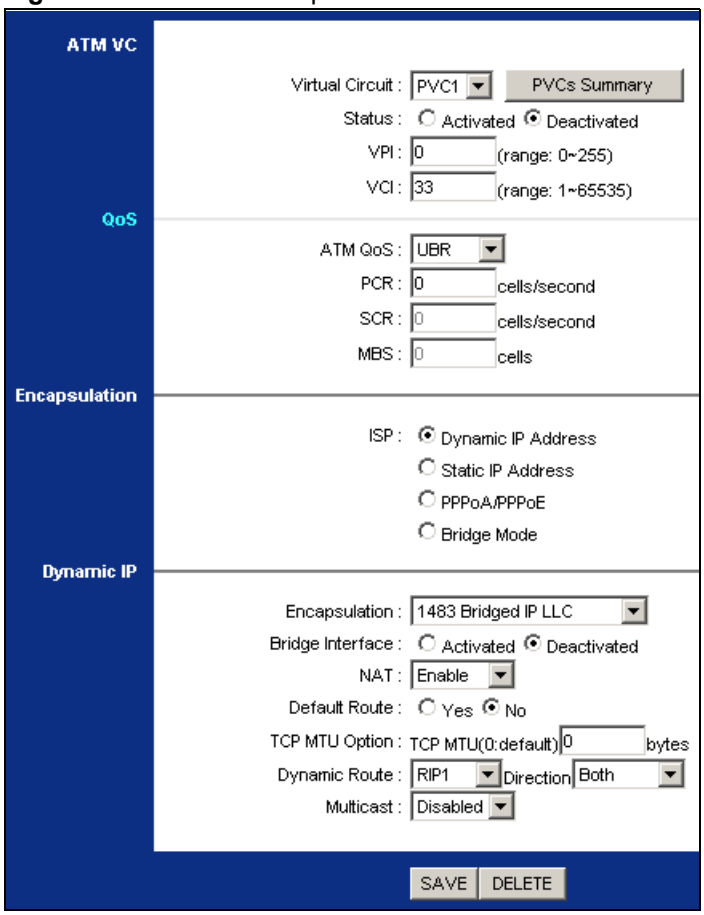
7.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

7.2 The Internet Screen

Use this screen to change your ZyXEL Device's WAN settings. Click **Interface Setup** > **Internet**. The screen differs by the encapsulation you select.

Figure 21 Interface Setup > Internet



The following table describes the labels in this screen.

Table 11 Interface Setup > Internet

LABEL	DESCRIPTION
ATM VC	
Virtual Circuit	Select the PVC you want to configure from the drop-down list box.
PVCs Summary	Click this to display a summary table of the PVC settings on your ZyXEL Device. See Section 7.2.5 on page 62 for more details.
Status	Use this field to enable or disable the PVC.
VPI	Virtual Path Identifier (VPI) defines a virtual circuit. Refer to the appendix for more information. Enter the VPI assigned to you.
VCI	Virtual Channel Identifier (VCI) defines a virtual circuit. Enter the VCI assigned to you. Refer to the appendix for more information.
QoS	

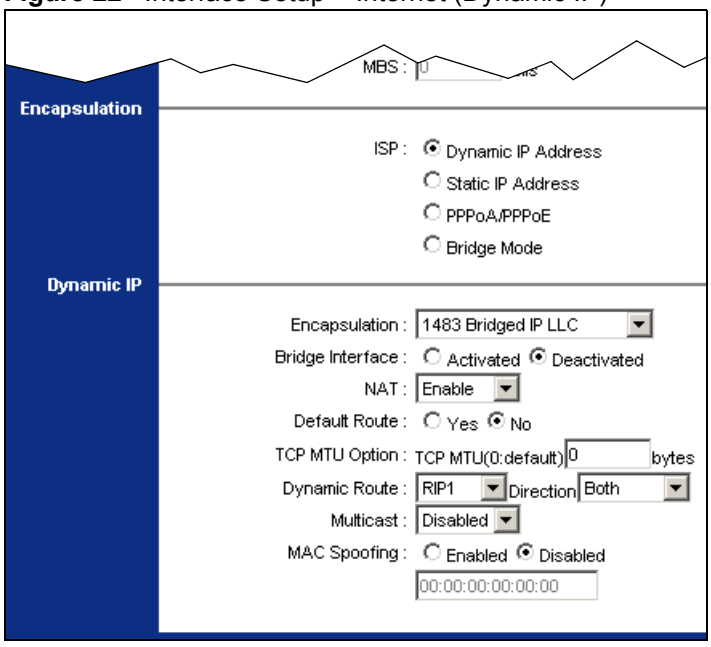
Table 11 Interface Setup > Internet (continued)

LABEL	DESCRIPTION
ATM QoS	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **rtVBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation. Select **nrtVBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.
PCR	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR in this field.
SCR	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
MBS	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Encapsulation	Select the connection type supported by your ISP. The next fields vary depending on what connection type you use. See the following sections for more details.
SAVE	Click this to save your changes.
DELETE	Click this to restore the PVC to default settings.

7.2.1 Dynamic IP Address

In the **Interface Setup** > **Internet** screen, select **Dynamic IP Address** from the **ISP** field to display the following screen.

Figure 22 Interface Setup > Internet (Dynamic IP)



The following table describes the labels in this screen.

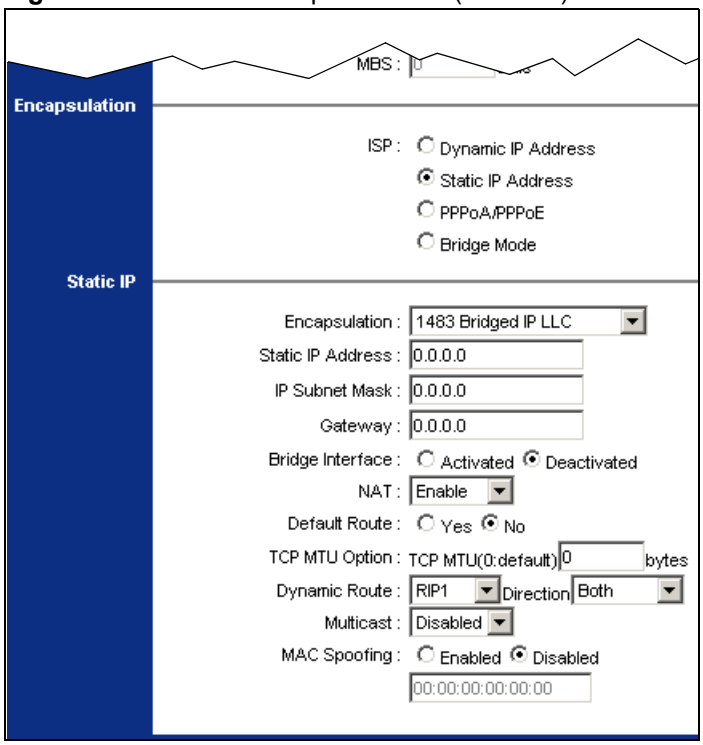
Table 12 Interface Setup > Internet (Dynamic IP)

LABEL	DESCRIPTION
Encapsulation	Select the method of multiplexing used by your ISP from the drop-down list box. Available options are: **1483 Bridged IP LLC**, **1483 Bridged IP VC-Mux**, **1483 Routed IP LLC(IPoA)** and **1483 Routed IP VC-Mux**.
Bridge Interface	This field is only available when you select **1483 Bridged IP LLC** or **1483 Bridged IP VC-Mux** in the **Encapsulation** field. Use this field to enable or disable the bridge mode. Activate the bridge mode when your ISP provides you with more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly.
NAT	Use this field to enable or disable Network Address Translation (NAT).
Default Route	Select **Yes** to direct traffic not listed in the routing table to the default gateway. Select **No** to drop traffic not listed in the routing table.
TCP MTU Option	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.
Dynamic Route	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Select the RIP version from **RIP1**, **RIP2-B** and **RIP2-M**.
Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP direction from **None**, **Both**, **IN Only** and **OUT Only**.
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). IGMP is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports **IGMP v1**, **IGMP v2** and **IGMP v3**. Select **Disabled** to turn off the feature.
MAC Spoofing	This field is only available when you select **1483 Bridged IP LLC** or **1483 Bridged IP VC-Mux** in the **Encapsulation** field. Use this field to alter the MAC address so that the PVCs on the ZyXEL Device can establish connections to the network.

7.2.2 Static IP Address

In the **Interface Setup** > **Internet** screen, select **Static IP Address** from the **ISP** field to display the following screen.

Figure 23 Interface Setup > Internet (Static IP)



The following table describes the labels in this screen.

Table 13 Interface Setup > Internet (Static IP)

LABEL	DESCRIPTION
Encapsulation	Select the method of multiplexing used by your ISP from the drop-down list box. Available options are: **1483 Bridged IP LLC**, **1483 Bridged IP VC-Mux**, **1483 Routed IP LLC(IPoA)** and **1483 Routed IP VC-Mux**.
Static IP Address	A static IP address is a fixed IP that your ISP gives you. Type your ISP assigned IP address in the field.
IP Subnet Mask	Enter a subnet mask in dotted decimal notation.
Gateway	Specify a gateway IP address (supplied by your ISP).
Bridge Interface	This field is only available when you select **1483 Bridged IP LLC** or **1483 Bridged IP VC-Mux** in the **Encapsulation** field. Use this field to enable or disable the bridge mode. Activate the bridge mode when your ISP provides you with more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly.
NAT	Use this field to enable or disable Network Address Translation (NAT).
Default Route	Select **Yes** to direct traffic not listed in the routing table to the default gateway. Select **No** to drop traffic not listed in the routing table.
TCP MTU Option	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.

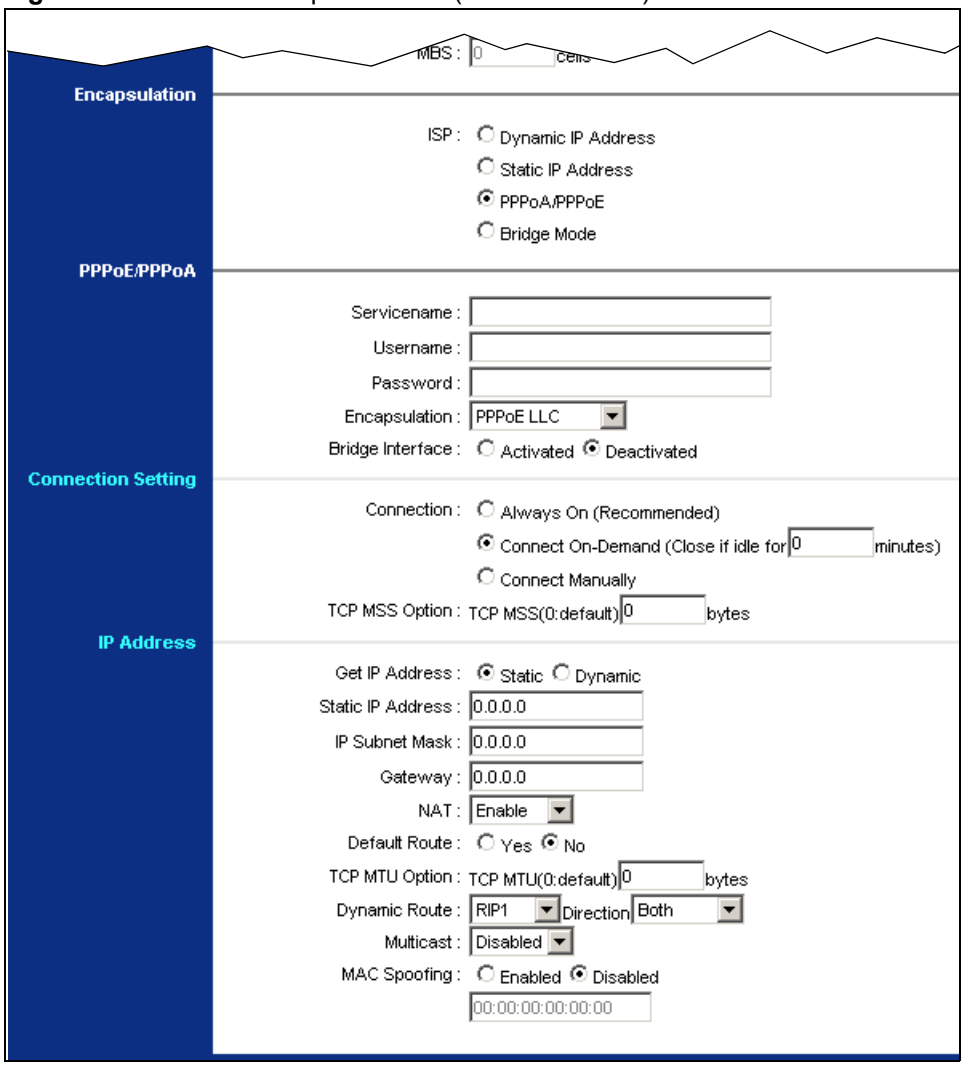
Table 13 Interface Setup > Internet (Static IP) (continued)

LABEL	DESCRIPTION
Dynamic Route	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Select the RIP version from **RIP1**, **RIP2-B** and **RIP2-M**.
Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP direction from **None**, **Both**, **IN Only** and **OUT Only**.
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). IGMP is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports **IGMP v1**, **IGMP v2** and **IGMP v3**. Select **Disabled** to turn off the feature.
MAC Spoofing	This field is only available when you select **1483 Bridged IP LLC** or **1483 Bridged IP VC-Mux** in the **Encapsulation** field. Use this field to alter the MAC address so that the PVCs on the ZyXEL Device can establish connections to the network.

7.2.3 PPPoA/PPPoE

In the **Interface Setup** > **Internet** screen, select **PPPoA/PPPoE** from the **ISP** field to display the following screen.

Figure 24 Interface Setup > Internet (PPPoA/PPPoE)



The following table describes the labels in this screen.

Table 14 Interface Setup > Internet (PPPoA/PPPoE)

LABEL	DESCRIPTION
PPPoE/PPPoA	
Servicename	Type the name of your service in this field.
Username	Enter the username exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the username above.
Encapsulation	Select the method of multiplexing used by your ISP from the drop-down list box. Available options are: **PPPoE LLC**, **PPPoE VC-Mux**, **PPPoA LLC** and **PPPoA VC-Mux**.

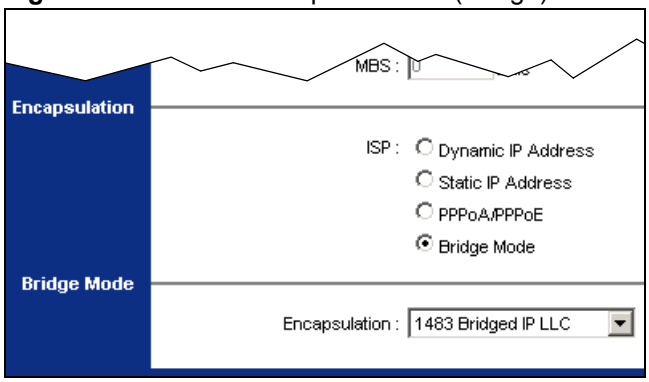
Table 14 Interface Setup > Internet (PPPoA/PPPoE) (continued)

LABEL	DESCRIPTION
Bridge Interface	This field is only available when you select **PPPoE LLC** or **PPPoE VC-Mux** in the **Encapsulation** field. Use this field to enable or disable the bridge mode. Activate the bridge mode when your ISP provides you with more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly.
Connection Setting	
Connection	Select **Always On (Recommended)** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected. Select **Connect On-Demand** when you don't want the connection up all the time and specify an idle time-out in minutes. The default setting is 0 minute, which means the Internet session will not timeout. Select **Connect Manually** to establish the connection only when you need it. Note: Do not specify an always-on connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.
TCP MSS Option	The TCP Maximum Segment Size (MSS) defines the size of the largest packet allowed on an interface or connection. Enter the TCP MSS in this field. In general, the TCP MSS is 1452.
IP Address	
Get IP Address	Select the type of IP address provided by your ISP. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Static IP Address	Type your ISP assigned IP address in the field.
IP Subnet Mask	Enter a subnet mask in dotted decimal notation.
Gateway	Specify a gateway IP address (supplied by your ISP).
NAT	Use this field to enable or disable Network Address Translation (NAT).
Default Route	Select **Yes** to direct traffic not listed in the routing table to the default gateway. Select **No** to drop traffic not listed in the routing table.
TCP MTU Option	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.
Dynamic Route	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Select the RIP version from **RIP1**, **RIP2-B** and **RIP2-M**.
Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP direction from **None**, **Both**, **IN Only** and **OUT Only**.
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). IGMP is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports **IGMP v1**, **IGMP v2** and **IGMP v3**. Select **Disabled** to turn off the feature.
MAC Spoofing	This field is only available when you select **1483 Bridged IP LLC** or **1483 Bridged IP VC-Mux** in the **Encapsulation** field. Use this field to alter the MAC address so that the PVCs on the ZyXEL Device can establish connections to the network.

7.2.4 Bridge Mode

In the **Interface Setup** > **Internet** screen, select **Bridge Mode** from the **ISP** field to display the following screen.

Figure 25 Interface Setup > Internet (Bridge)



The following table describes the labels in this screen.

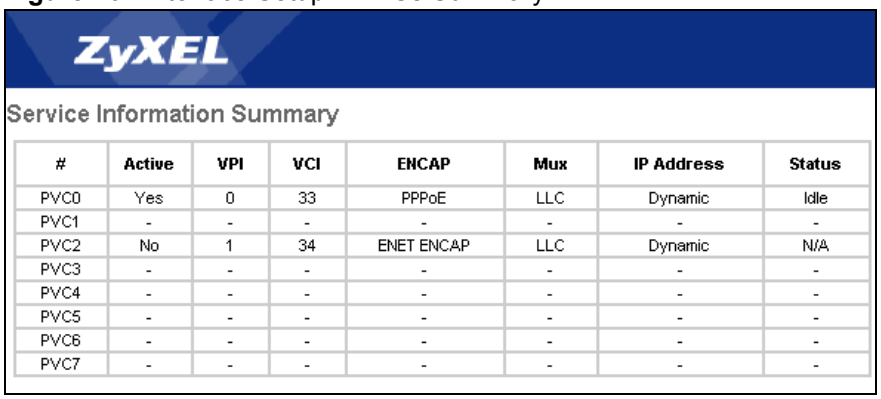
Table 15 Interface Setup > Internet (Bridge)

LABEL	DESCRIPTION
Encapsulation	Select the method of multiplexing used by your ISP from the drop-down list box. Available options are: **1483 Bridged IP LLC** and **1483 Bridged IP VC-Mux**.

7.2.5 The PVCs Summary Screen

Use this field to check your PVC settings. In the **Interface Setup** > **Internet** screen, click **PVCs Summary** in the **Virtual Circuit** field to display the following screen.

Figure 26 Interface Setup > PVCs Summary



#	Active	VPI	VCI	ENCAP	Mux	IP Address	Status
PVC0	Yes	0	33	PPPoE	LLC	Dynamic	Idle
PVC1	-	-	-	-	-	-	-
PVC2	No	1	34	ENET ENCAP	LLC	Dynamic	N/A
PVC3	-	-	-	-	-	-	-
PVC4	-	-	-	-	-	-	-
PVC5	-	-	-	-	-	-	-
PVC6	-	-	-	-	-	-	-
PVC7	-	-	-	-	-	-	-

The following table describes the labels in this screen.

Table 16 Interface Setup > PVCs Summary

LABEL	DESCRIPTION
#	This field displays the index number for the corresponding PVC.
Active	This field displays whether the PVC is activated.
VPI	This field displays the VPI value.
VCI	This field displays the VCI value.

Table 16 Interface Setup > PVCs Summary (continued)

LABEL	DESCRIPTION
ENCAP	This field displays the type of encapsulation.
Mux	This field displays the multiplexing method.
IP Address	This field displays the type of IP address.
Status	This field displays the connection status of the PVC.

7.3 WAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

7.3.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device supports the following methods.

PPP over Ethernet

The ZyXEL Device supports Point-to-Point Protocol over Ethernet (PPPoE). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

7.3.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

7.3.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

7.3.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. However the encapsulation method assigned influences your choices for IP address.

IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the **IP Address** field and not the **Gateway IP Address** field.

IP Assignment with RFC 1483 Encapsulation

In this case the IP address assignment must be static.

7.3.5 Always-On Connection (PPP)

An always-on connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyXEL Device does two things when you specify an always-on connection. The first is that idle timeout is disabled. The second is that the ZyXEL Device will try to bring up the connection when turned on and whenever the connection is down. An always-on connection can be very expensive for obvious reasons.

Do not specify an always-on connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

7.3.6 ATM QoS

ATM QoS is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

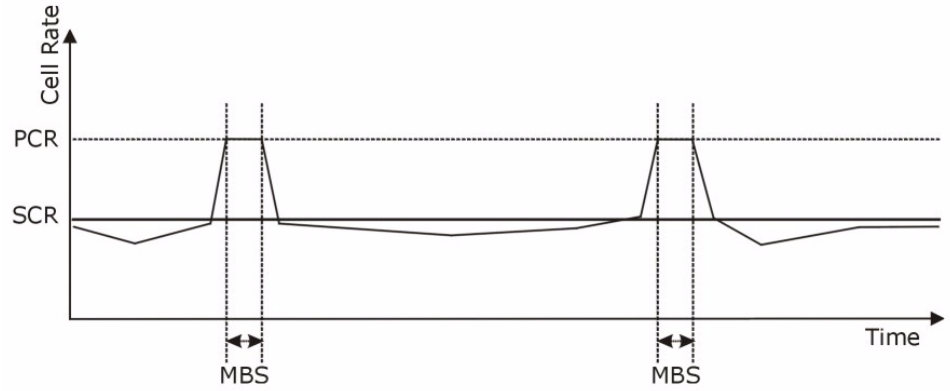
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 27 Example of ATM OoS



7.3.7 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

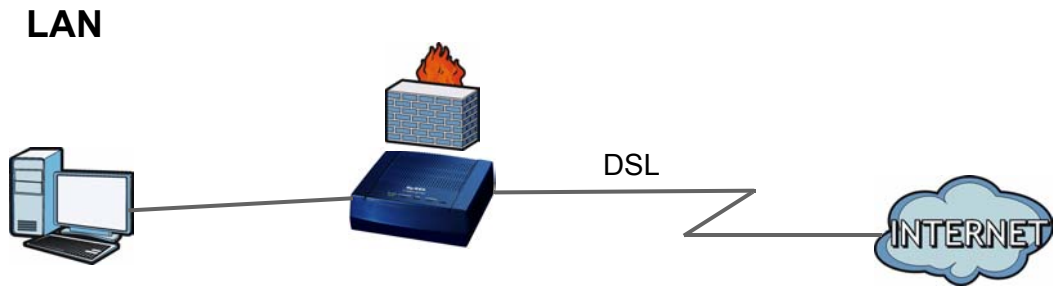
8

LAN Setup

8.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one area such as a building or floor of a building.

Use the LAN screen to help you configure a LAN DHCP server and manage IP addresses.



8.1.1 What You Can Do in the LAN Screens

- Use the **LAN** screen (Section 8.2 on page 68) to set the LAN IP address and subnet mask of your ZyXEL device. You can also edit your ZyXEL Device's RIP, multicast and DHCP settings from this screen.
- Use the **DHCP IP Pool Summary** screen (Section 8.2.1 on page 70) to check the IP and MAC addresses of the computers on your LAN.

8.1.2 What You Need To Know About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your ZyXEL Device an IP address, subnet mask, DNS and other routing information when it's turned on.

RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 is an improvement over version 1, but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network.

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

Finding Out More

See Section 8.3 on page 71 for technical background information on LANs.

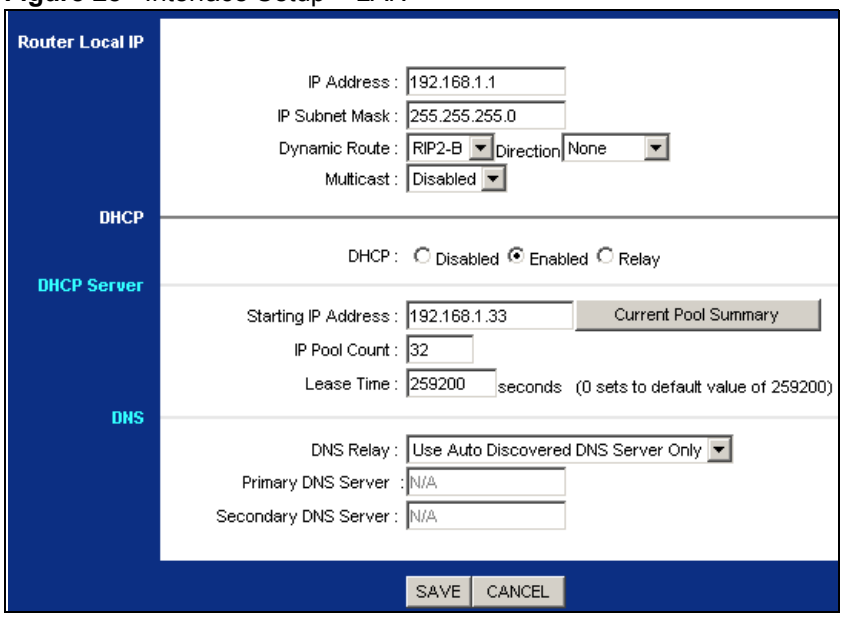
8.2 The LAN Screen

Use this screen to configure your LAN settings. Click **Interface Setup > LAN** to display the following screen.

Follow these steps to configure your LAN settings.

1. Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your ZyXEL Device.
2. Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
3. Click **SAVE** to save your settings.

Figure 28 Interface Setup > LAN


Router Local IP
IP Address : 192.168.1.1
IP Subnet Mask : 255.255.255.0
Dynamic Route : RIP2-B Direction None
Multicast : Disabled
DHCP
DHCP : Disabled Enabled Relay
DHCP Server
Starting IP Address : 192.168.1.33
Current Pool Summary
IP Pool Count : 32
Lease Time : 259200 seconds (0 sets to default value of 259200)
DNS
DNS Relay : Use Auto Discovered DNS Server Only
Primary DNS Server : N/A
Secondary DNS Server : N/A
SAVE
CANCEL

The following table describes the fields in this screen.

Table 17 Interface Setup > LAN

LABEL	DESCRIPTION
Router Local IP	
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your ZyXEL Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
Dynamic Route	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Select the RIP version from **RIP1**, **RIP2-B** and **RIP2-M**.
Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP direction from **None**, **Both**, **IN Only** and **OUT Only**.
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). IGMP is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports **IGMP v1**, **IGMP v2** and **IGMP v3**. Select **Disabled** to turn off the feature.
DHCP	
DHCP	If set to **Enabled**, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to operating systems that support the DHCP client. If set to **Disabled**, the DHCP server will be disabled. If set to **Relay**, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
DHCP Server	
Starting IP Address	This field specifies the first of the contiguous addresses in the IP address pool.

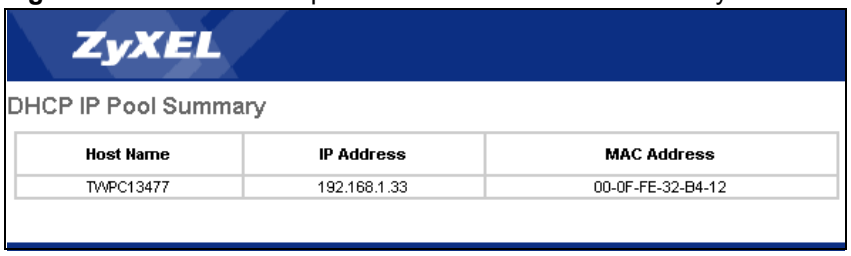
Table 17 Interface Setup > LAN

LABEL	DESCRIPTION
Current Pool Summary	Click this to display a summary table for the IP address pool. See Section 8.2.1 on page 70 for more details. The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.
IP Pool Count	This field specifies the size, or count of the IP address pool.
Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
DNS	
DNS Relay	Select **Auto Discovered DNS Server Only** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select **User Discovered DNS Server Only** if you have the IP address of a DNS server. You have to specify the primary and secondary DNS servers in the following fields.
Primary DNS Server	Enter the IP address for the primary DNS server.
Secondary DNS Server	Enter the IP address for the secondary DNS server.
DHCP Server IP for Relay Agent	This field is only available when you select **Relay** in the **DNS Relay** field. Enter the IP address of the actual remote DHCP server in this field.
SAVE	Click this to save your changes.
CANCEL	Click this to restore your previously saved settings.

8.2.1 The DHCP IP Pool Summary Screen

This table allows you to see the IP and Media Access Control (MAC) addresses of individual computers on your LAN. In the **Interface Setup > LAN** screen, click the **Current Pool Summary** button to open the following screen.

Figure 29 Interface Setup > LAN > DHCP IP Pool Summary



The following table describes the labels in this screen.

Table 18 Interface Setup > LAN > DHCP IP Pool Summary

LABEL	DESCRIPTION
Host Name	This field displays the name of a computer that receives an IP address from the ZyXEL Device.
IP Address	This field displays the IP address of a computer that receives an IP address from the ZyXEL Device.
MAC Address	This field displays the MAC address of a computer that receives an IP address from the ZyXEL Device.

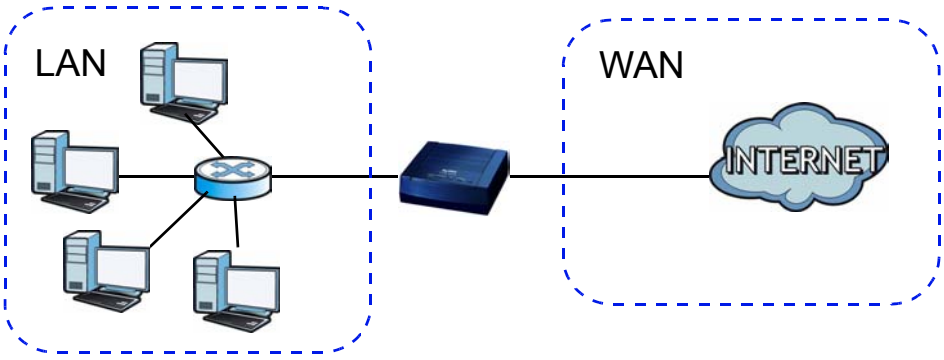
8.3 LAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

8.3.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 30 LAN and WAN IP Addresses



8.3.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

8.3.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **Primary** and **Secondary DNS Server** fields.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

  If the DHCP is set to **Relay**, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device acts as a DNS proxy and forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses.

8.3.4 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

8.3.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both -** the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only -** the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only -** the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None -** the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

8.3.6 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports IGMP version 1 (**IGMP-v1**), IGMP version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

PART V
Advanced Setup

Static Route (77)
Network Address Translation (NAT) (81)
Quality of Service (QoS) (91)
ADSL (99)
Firewall (101)

9

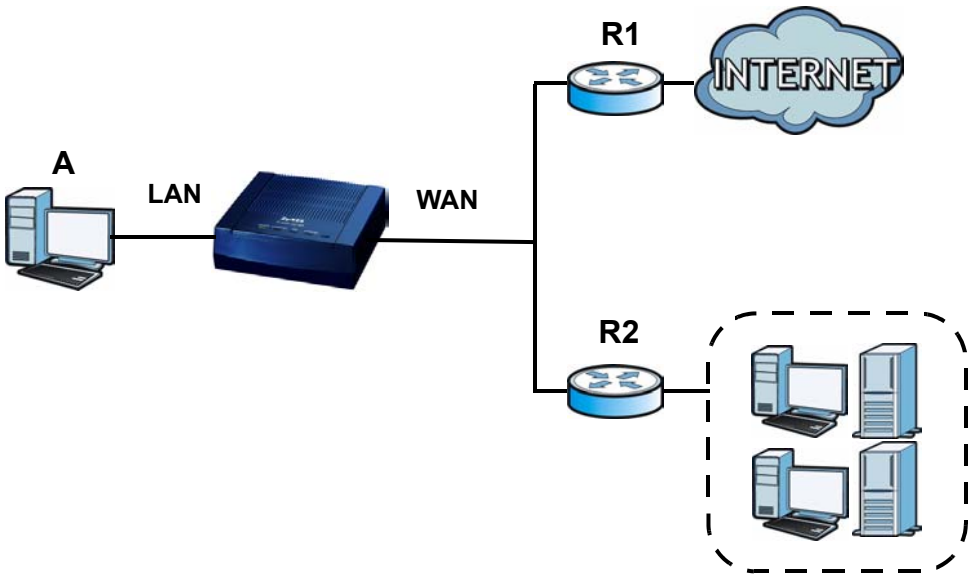
Static Route

9.1 Overview

The ZyXEL Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the ZyXEL Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**.

Figure 31 Example of Static Routing Topology



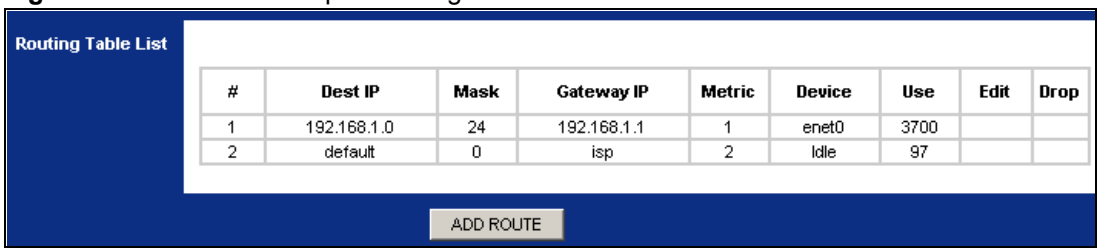
9.1.1 What You Can Do in the Static Route Screens

- Use the **Routing Table List** screen (Section 9.2 on page 78) to view static routes on the ZyXEL Device.
- Use the **Static Route** screen (Section 9.2.1 on page 78) to add or edit IP static routes on the ZyXEL Device.

9.2 The Routing Table List Screen

Use this screen to view the static route rules. Click **Advanced Setup > Routing** to display the following screen.

Figure 32 Advanced Setup > Routing Table List


Routing Table List
Dest IP Mask Gateway IP Metric Device Use Edit Drop
1 192.168.1.0 24 192.168.1.1 1 enet0 3700
2 default 0 isp 2 Idle 97
ADD ROUTE

The following table describes the labels in this screen.

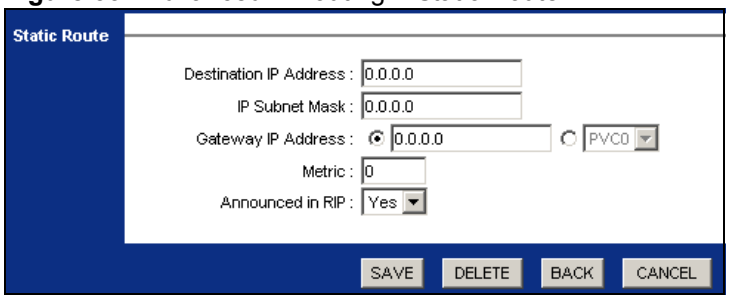
Table 19 Advanced Setup > Routing Table List

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Dest IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Mask	This parameter specifies the IP network subnet mask of the final destination.
Gateway IP	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	This field displays the priority of each route on the ZyXEL Device.
Device	This is the name that describes or identifies this route.
Use	This is the number of times the route was used.
Edit	Click this to go to the screen where you can set up a static route on the ZyXEL Device. You cannot edit the default routes.
Drop	Click this to remove a static route from the ZyXEL Device. You cannot delete the default routes.
ADD ROUTE	Click this to add a new static route on the ZyXEL Device.

9.2.1 The Static Route Screen

Use this screen to configure the required information for a static route. Select a static route index number and click **Edit**, or click the **ADD ROUTE** button in the **Routing Table List** screen. The screen shown next appears.

Figure 33 Advanced > Routing > Static Route


Static Route
Destination IP Address : 0.0.0.0
IP Subnet Mask : 0.0.0.0
Gateway IP Address : 0.0.0.0 PVC0
Metric : 0
Announced in RIP : Yes
SAVE DELETE BACK CANCEL

The following table describes the labels in this screen.

Table 20 Advanced > Static Route: Edit

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	You can set the static route using a gateway IP address or a remote node. Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Select a remote node from the drop-down list box to set the static route. A remote note is a connection point outside of the local area network. One example of a remote node is your connection to your ISP. See Section 7.2 on page 55 for details on configuring a remote node.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Announced in RIP	Routing Information Protocol (RIP) allows a router to exchange routing information with other routers. Select **Yes** to allow RIP to send information about the static route to other routers. Select **No** to prevent RIP from sending information about the static route to other routers.
SAVE	Click this to save your changes.
DELETE	Click this to remove the static route.
BACK	Click this to return to the previous screen without saving.
CANCEL	Click this to restore your previously saved settings.

10

Network Address Translation (NAT)

10.1 Overview

This chapter discusses how to configure NAT on the ZyXEL Device. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

10.1.1 What You Can Do in the NAT Screens

- Use the **NAT** screen (Section 10.2 on page 82) to configure the NAT settings.
- Use the **DMZ** screen (Section 10.3 on page 83) to configure the DMZ settings.
- Use the **Virtual Server** screen (Section 10.4 on page 84) to forward incoming service requests to the server(s) on your local network.
- Use the **IP Address Mapping** screen (Section 10.5 on page 86) to change your ZyXEL Device's address mapping settings.

10.1.2 What You Need To Know About NAT

Inside/Outside

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Public/Local

Public/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the public address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Single IP Versus NAT

Single IP is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports multiple IPs to map multiple public IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

- Choose **Single IP** if you have just one public WAN IP address for your ZyXEL Device.
- Choose **Multiple IPs** if you have multiple public WAN IP addresses for your ZyXEL Device.

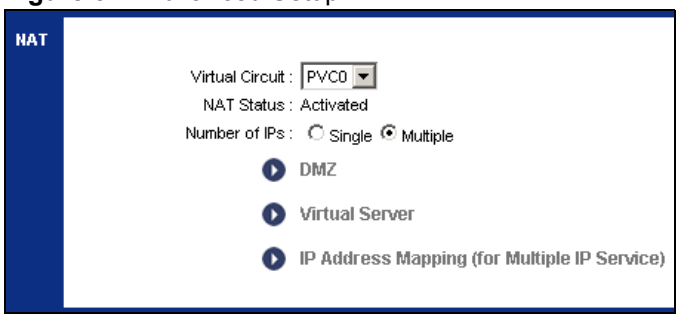
Finding Out More

See Section 10.6 on page 88 for advanced technical information on NAT.

10.2 The NAT Screen

Use this screen to configure NAT for each PVC. Click **Advanced Setup > NAT** to open the following screen.

Figure 34 Advanced Setup > NAT



The following table describes the labels in this screen.

Table 21 Network > NAT > General

LABEL	DESCRIPTION
Virtual Circuit	Select the PVC you want to configure from the drop-down list box.
NAT Status	This field shows whether NAT is enabled. See Section 7.2 on page 55 for more details on activating NAT.

Table 21 Network > NAT > General (continued)

LABEL	DESCRIPTION
Number of IPs	Select **Single** if you have just one public WAN IP address for your ZyXEL Device. Select **Multiple** if you have multiple public WAN IP addresses for your ZyXEL Device.
DMZ	Click this to configure the DMZ settings. See Section 10.3 on page 83 for more details.
Virtual Server	Click this to configure port forwarding rules for your ZyXEL Device. See Section 10.4 on page 84 for more details.
IP Address Mapping	This is available only when you select **Multiple** in the **Number of IPs** field. Click this to configure address mapping rules for your ZyXEL Device. See Section 10.5 on page 86 for more details.

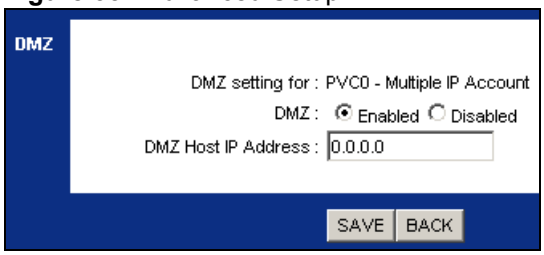
10.3 The DMZ Screen

The DeMilitarized Zone (DMZ) provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

Use this screen to configure a separate independent network from the LAN in which you can put your servers. Click **Advanced Setup > NAT** > **DMZ** to open the following screen.

Figure 35 Advanced Setup > NAT > DMZ



The following table describes the labels in this screen.

Table 22 Advanced Setup > NAT > DMZ

LABEL	DESCRIPTION
DMZ setting for	This field displays the PVC you want to configure.
DMZ	Use this field to enable or disable DMZ.
DMZ Host IP Address	Type the IP address for DMZ in dotted decimal notation. Note: Make sure the IP addresses of the LAN, WAN and DMZ are on separate subnets.
SAVE	Click this to save your settings.
BACK	Click this to return to the previous screen without saving.

10.4 The Virtual Server Screen

LAN computers usually have DHCP-assigned private IP address that cannot be accessed directly from the WAN. Use this screen to allow the ZyXEL Device to forward traffic to the servers on the LAN.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

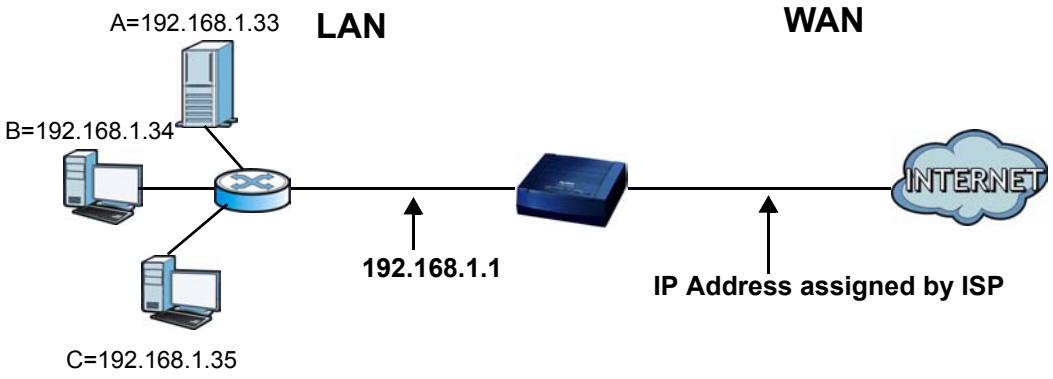
The most often used port numbers and services are shown in Appendix D on page 205. Please refer to RFC 1700 for further information about port numbers.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

10.4.1 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 36 Multiple Servers Behind NAT Example



The following table summarizes the settings described in the above example.

Table 23 Multiple Servers Behind NAT Example

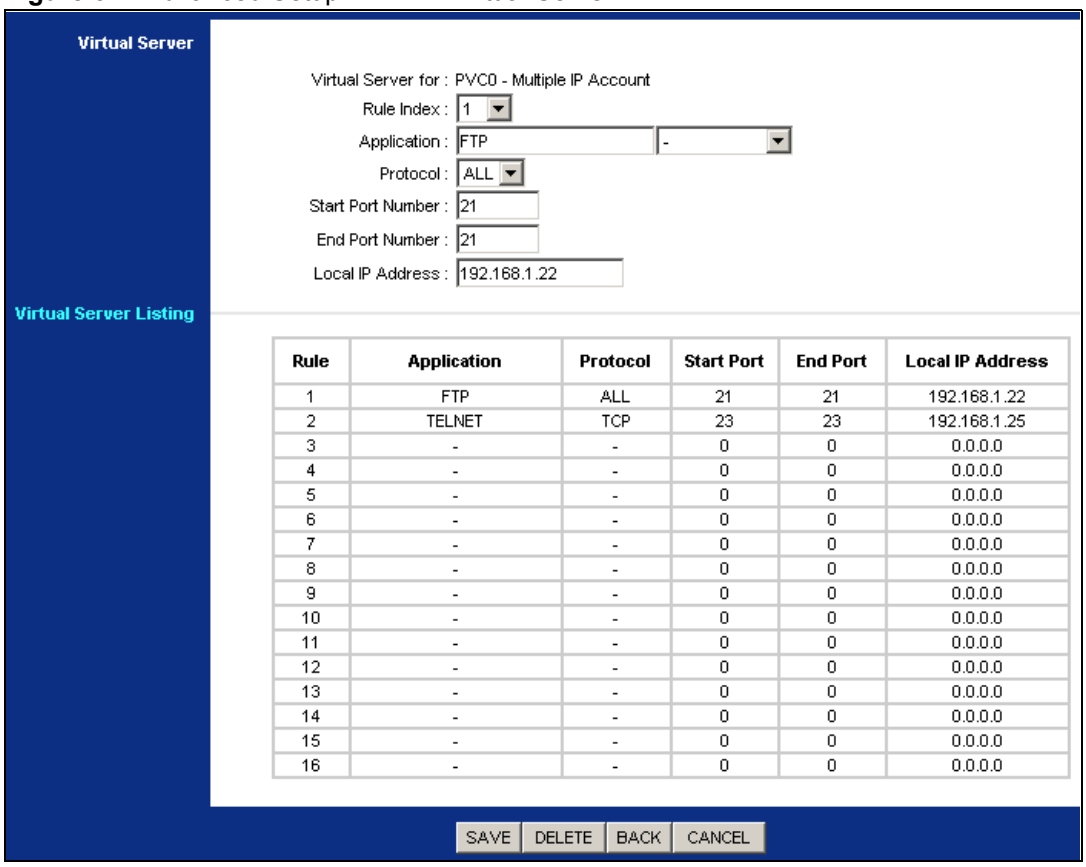
	SERVERS	PORTS	DEFAULT SERVER IP
A	FTP	21-22	192.168.1.33
B	Telnet	23	192.168.1.34
C	SMTP	25	192.168.1.35

10.4.2 Configuring the Virtual Server Screen

Click **Advanced Setup > NAT > Virtual Server** to open the following screen.

See Appendix D on page 205 for port numbers commonly used for particular services.

Figure 37 Advanced Setup > NAT > Virtual Server


Virtual Server
Virtual Server for : PVC0 - Multiple IP Account
Rule Index : 1
Application : FTP -
Protocol : ALL
Start Port Number : 21
End Port Number : 21
Local IP Address : 192.168.1.22
Virtual Server Listing
Rule Application Protocol Start Port End Port Local IP Address
1 FTP ALL 21 21 192.168.1.22
2 TELNET TCP 23 23 192.168.1.25
3 - - 0 0 0.0.0.0
4 - - 0 0 0.0.0.0
5 - - 0 0 0.0.0.0
6 - - 0 0 0.0.0.0
7 - - 0 0 0.0.0.0
8 - - 0 0 0.0.0.0
9 - - 0 0 0.0.0.0
10 - - 0 0 0.0.0.0
11 - - 0 0 0.0.0.0
12 - - 0 0 0.0.0.0
13 - - 0 0 0.0.0.0
14 - - 0 0 0.0.0.0
15 - - 0 0 0.0.0.0
16 - - 0 0 0.0.0.0
SAVE
DELETE
BACK
CANCEL

The following table describes the fields in this screen.

Table 24 Advanced Setup > NAT > Virtual Server

LABEL	DESCRIPTION
Virtual Server	
Virtual Server for	This is the PVC that this virtual server will use.
Rule Index	Select the rule's index number from the drop-down list box.
Application	Use the drop-down list box to select the type of server you have on your network. Applications or services are defined by their protocol (TCP or UDP) and port number. For example, TCP port 80 defines web (HTTP) traffic. If you have a web server on your network, you need to forward HTTP applications (TCP port 80) to the server's IP address. Choices are: **FTP**, **SSH**, **TELNET**, **SMTP**, **HTTP_Server**, **POP3**, **HTTPS**, **T.120**, **H.323**, **PPTP**, **pcAnywhere**, **VNC** and **CUSeeMe**.
Protocol	Use the drop-down list box to choose the IP port (**ALL**, **TCP** or **UDP**) that defines your service.

Table 24 Advanced Setup > NAT > Virtual Server

LABEL	DESCRIPTION
Start Port Number	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port Number** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port Number** field.
End Port Number	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port Number** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port Number** field above.
Local IP Address	Enter the inside IP address of the server in this field.
Virtual Server Listing	
Rule	This is the rule's index number.
Application	This is a service's name.
Protocol	This is the IP port.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Local IP Address	This is the server's IP address.
SAVE	Click this to save your changes.
DELETE	Click this to remove the rule.
BACK	Click this to return to the previous screen without saving.
CANCEL	Click this to restore your previously saved settings.

10.5 The IP Address Mapping Screen

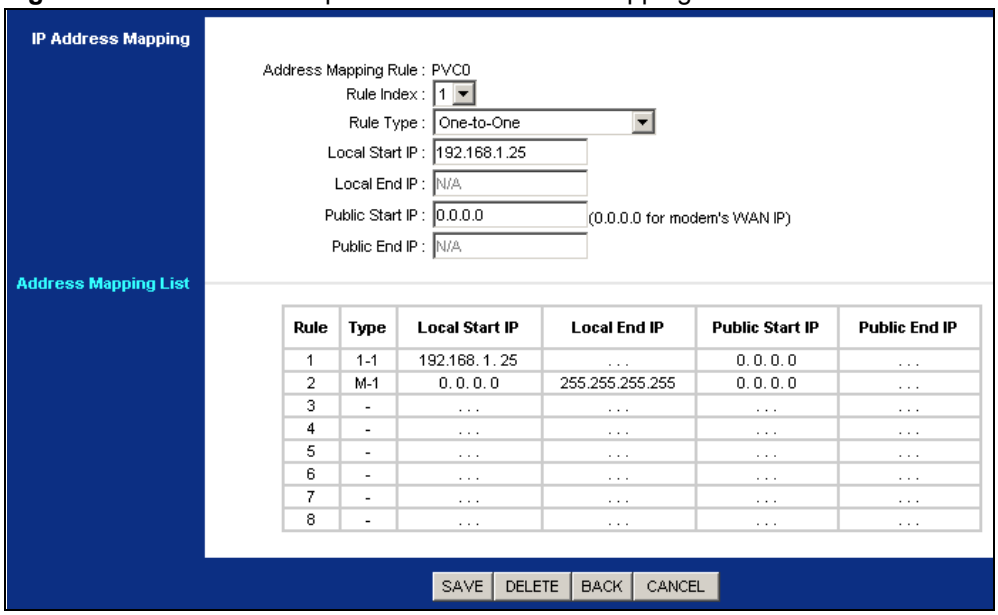
Configure this screen if you have multiple IP addresses from your ISP and you want to map them to private IP addresses on your LAN.

The **Address Mapping** screen is available only when you select **Multiple** for the **Number of IPs** in the **NAT** screen.

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored.

Use this screen to change your ZyXEL Device's address mapping settings. Click **Advanced Setup > NAT > IP Address Mapping** to open the following screen.

Figure 38 Advanced Setup > NAT > IP Address Mapping


IP Address Mapping
Address Mapping Rule : PVC0
Rule Index : 1
Rule Type : One-to-One
Local Start IP : 192.168.1.25
Local End IP : N/A
Public Start IP : 0.0.0.0 (0.0.0.0 for modem's WAN IP)
Public End IP : N/A
Address Mapping List
Rule Type Local Start IP Local End IP Public Start IP Public End IP
1 1-1 192.168.1.25 ... 0.0.0.0 ...
2 M-1 0.0.0.0 255.255.255.255 0.0.0.0 ...
3 - ... ...
4 - ... ...
5 - ... ...
6 - ... ...
7 - ... ...
8 - ... ...
SAVE
DELETE
BACK
CANCEL

The following table describes the fields in this screen.

Table 25 Network > NAT > Address Mapping

LABEL	DESCRIPTION
IP Address Mapping	
Address Mapping Rule	The rules configured in this screen apply to this PVC.
Rule Index	Select the rule's index number from the drop-down list box.
Rule Type	Choose the port mapping type from one of the following. **One-to-One**: This mode maps one local IP address to one public IP address. Note that port numbers do not change for one-to-one NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one public IP address. This is equivalent to the **Single IP** feature that previous ZyXEL routers supported only. **Many-to-Many Overload**: This mode maps multiple local IP addresses to shared public IP addresses. **Many-to-Many No Overload**: This mode maps each local IP address to unique public IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address. If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Public Start IP	This is the starting public IP address. Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Public End IP	This is the ending public IP address. This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.

Table 25 Network > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Address Mapping List	
Rule	This is the rule's index number.
Type	**1-1**: One-to-One mode maps one local IP address to one public IP address. Note that port numbers do not change for the One-to-One NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one public IP address. This is equivalent to the **Single IP** feature that previous ZyXEL routers supported only. **M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared public IP addresses. **MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique public IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting inside local IP address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the ending inside local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Public Start IP	This is the starting inside public IP address. Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Public End IP	This is the ending inside public IP address. This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.
SAVE	Click this to save your changes.
DELETE	Click this to remove the rule.
BACK	Click this to return to the previous screen without saving.
CANCEL	Click this to restore your previously saved settings.

10.6 NAT Technical Reference

This section contains more information regarding NAT.

10.6.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Public/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the public address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while public/local refers to the IP address of a host used in a packet. Thus, an inside local address is the IP address of an inside host in a packet when the packet is still in the local network, while an inside public address is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 26 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Public	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or public) of an outside host.

10.6.2 What NAT Does

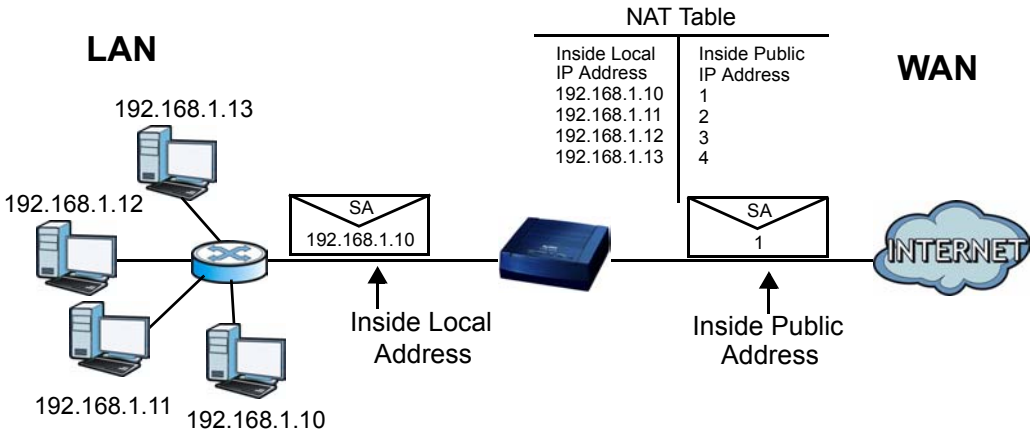
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside public address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside public address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or public) of an outside host is never changed.

The public IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network.

10.6.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the inside local address is the source address on the LAN, and the inside public address is the source address on the WAN. For incoming packets, the inside local address is the destination address on the LAN, and the inside public address is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 39 How NAT Works



11

Quality of Service (QoS)

11.1 Overview

Use the **QoS** screen to set up your ZyXEL Device to use QoS for traffic management.

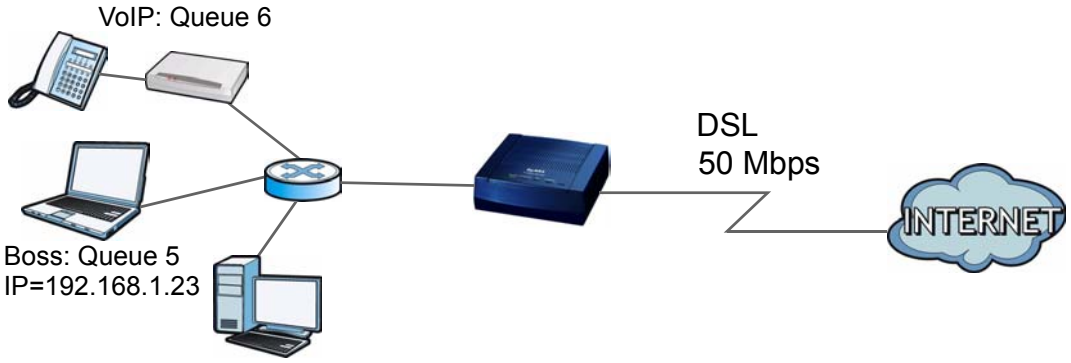
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data are equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

The ZyXEL Device assigns each packet a priority and then queues the packet accordingly. Packets assigned with a high priority are processed more quickly than those with low priorities if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 5. Traffic that does not match these two classes are assigned priority queue based on the internal QoS mapping table on the ZyXEL Device.

Figure 40 QoS Example



11.1.1 What You Can Do in the QoS Screens

- Use the **QoS** screen (Section 11.2 on page 93) to configure QoS settings on the ZyXEL Device.
- Use the **QoS Settings Summary** screen (Section 11.2.1 on page 95) to check the summary of QoS rules and actions you configured for the ZyXEL Device.

11.1.2 What You Need to Know About QoS

802.1p

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. 802.1p is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use 802.1p to give different priorities to different packet types.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DiffServ Code Point (DSCP) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Finding Out More

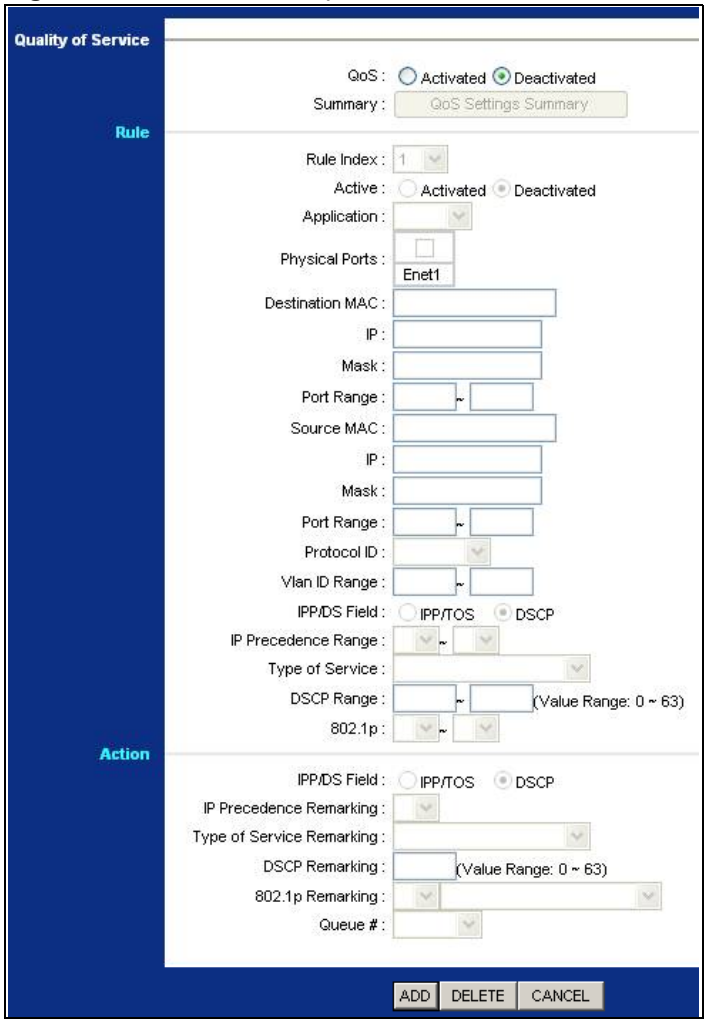
See Section 11.3 on page 96 for advanced technical information on QoS.

11.2 The QoS Screen

Use this screen to enable or disable QoS and have the ZyXEL Device assign priority levels to traffic according to the port range, IEEE 802.1p priority level and/or IP precedence.

Click **Advanced Setup > QoS** to open the screen as shown next.

Figure 41 Advanced Setup > QoS



The following table describes the labels in this screen.

Table 27 Advanced Setup > QoS

LABEL	DESCRIPTION
Quality of Service	
QoS	Use this field to turn on QoS to improve your network performance. You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
Summary	Click this to open a summary table showing the QoS settings. See Section 11.2.1 on page 95 for more details.
Rule	

Table 27 Advanced Setup > QoS

LABEL	DESCRIPTION
Rule Index	Select the rule's index number from the drop-down list box.
Active	Use this field to enable or disable the rule.
Application	Select an application from the drop-down list box. The **Destination Port Range** and **Protocol ID** fields may change depending on the type of applications you choose.
Physical Ports	Select **Enet1** to apply the rule to the Ethernet port.
Destination MAC	Type a destination MAC address here. QoS is then applied to traffic containing this destination MAC address. Leave it blank to apply the rule to all MAC addresses.
IP	Enter a destination IP address in dotted decimal notation. QoS is then applied to traffic containing this destination IP address. A blank destination IP address means any destination IP address.
Mask	Enter a destination subnet mask here.
Port Range	Either use the default value set by the application you choose, or enter the port number to which the rule should be applied.
Source MAC	Type a source MAC address here. QoS is then applied to traffic containing this source MAC address. Leave it blank to apply the rule to all MAC addresses.
IP	Enter a source IP address in dotted decimal notation. QoS is then applied to traffic containing this source IP address. A blank source IP address means any source IP address.
Mask	Enter a source subnet mask here.
Port Range	Enter the port number to which the rule should be applied. 0 means any source port number. See Appendix D on page 205 for some common services and port numbers.
Protocol ID	Select an IP protocol type from the drop-down list box.
Vlan ID Range	Enter the source VLAN ID in this field.
IPP/DS Field	Select **IPP/TOS** to specify an IP precedence range and type of services. Select **DSCP** to specify a DiffServ Code Point (DSCP) range.
IP Precedence Range	Enter a range from 0 to 7 for IP precedence. Zero is the lowest priority and seven is the highest.
Type of Service	Select a type of service from the drop-down list box. Available options are: **Normal service**, **Minimize delay**, **Maximize throughput**, **Maximize reliability** and **Minimize monetary cost**.
DSCP Range	Specify a DSCP number between 0 and 63 in this field.
802.1p	Select a priority level (0 to 7) from the drop-down list box.
Action	
IPP/DS Field	Select **IPP/TOS** to specify an IP precedence range and type of services. Select **DSCP** to specify a DiffServ Code Point (DSCP) range.
IP Precedence Remarking	Enter a range from 0 to 7 to re-assign IP precedence to matched traffic. Zero is the lowest priority and seven is the highest.
Type of Service Remarking	Select a type of service to re-assign the priority level to matched traffic. Available options are: **Normal service**, **Minimize delay**, **Maximize throughput**, **Maximize reliability** and **Minimize monetary cost**.
DSCP Remarking	Specify a DSCP number between 0 and 63 to re-assign the priority level to matched traffic.
802.1p Remarking	Select a priority level (0 to 7) to re-assign the priority level to matched traffic.

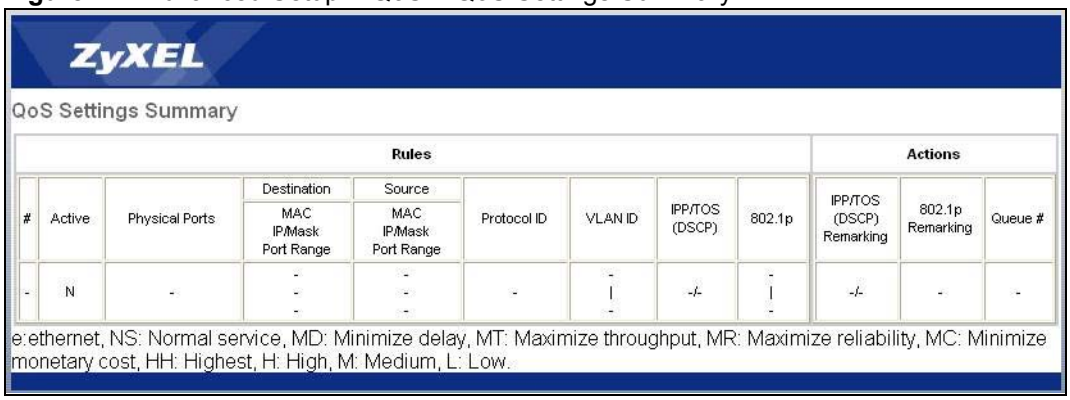
Table 27 Advanced Setup > QoS

LABEL	DESCRIPTION
Queue #	Specify a **Low**, **Medium**, **High** or **Highest** queue tag to matched traffic. Traffic assigned to a higher queue gets through faster while traffic in lower queues is dropped when there is network congestion.
ADD	Click this to add the rule.
DELETE	Click this to remove the rule.
CANCEL	Click this to restore previously saved settings.

11.2.1 The QoS Settings Summary Screen

Use this screen to display a summary of rules and actions configured for the ZyXEL Device. In the **Advanced > QoS** screen, click the **QoS Settings Summary** button to open the following screen.

Figure 42 Advanced Setup > QoS > QoS Settings Summary



The following table describes the labels in this screen.

Table 28 Advanced Setup > QoS > QoS Settings Summary

LABEL	DESCRIPTION
Rules	
#	This is the rule's index number.
Active	This shows whether the rule is enabled or disabled.
Physical Ports	This is the physical port associated with the rule.
Destination MAC and IP/Mask Port Ranges	This is the port range for destination MAC address and IP address.
Source MAC and IP/Mask Port Ranges	This is the port range for source MAC address and IP address.
Protocol ID	This is the protocol ID associated with the rule.
VLAN ID	This is the VLAN ID associated with the rule.
IPP/TOS (DSCP)	This shows the IPP/TOS or DSCP settings.
802.1p	This is the 802.1p priority level.
Actions	

Table 28 Advanced Setup > QoS > QoS Settings Summary (continued)

LABEL	DESCRIPTION
IPP/TOS (DSCP) Remarking	The ZyXEL Device re-assigns the priority values specified in this field to matched traffic.
802.1p Remarking	The ZyXEL Device re-assigns the priority levels specified in this field to matched traffic.
Queue #	The ZyXEL Device assigns the queue level specified in this field to matched traffic.

11.3 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

11.3.1 IEEE 802.1p

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 29 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

11.3.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

11.3.3 Automatic Priority Queue Assignment

If you enable QoS on the ZyXEL Device, the ZyXEL Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the ZyXEL Device. On the ZyXEL Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 30 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000 111000	
		7		

12 ADSL

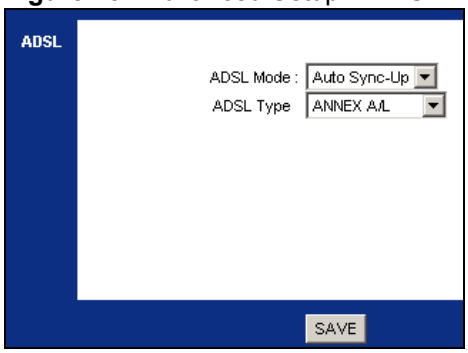
12.1 Overview

This chapter contains information about configuring the ADSL settings for your ZyXEL Device.

12.2 The ADSL Screen

Use this screen to select the ADSL mode and type for your ZyXEL Device. Click **Advanced Setup > ADSL** to open the following screen.

Figure 43 Advanced Setup > ADSL



The following table describes the labels in this screen.

Table 31 Advanced Setup > ADSL

LABEL	DESCRIPTION
ADSL Mode	Select the mode supported by your ISP. Use **Auto Sync-Up** if you are not sure which mode to choose from. The ZyXEL Device dynamically diagnoses the mode supported by the ISP and selects the best compatible one for your connection. Other options are **ADSL2+**, **ADSL2**, **G.DMT**, **T1.413** and **G.lite**.
ADSL Type	Select the type supported by your ISP. Available options are **ANNEX A**, **ANNEX A/L**, **ANNEX M** and **ANNEX A/L/M**.
SAVE	Click this to save your changes.

13 Firewall

13.1 Overview

This chapter shows you how to enable the ZyXEL Device firewall. Use the firewall to protect your ZyXEL Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.
- blocks SYN and port scanner attacks.

By default, the ZyXEL Device blocks DDOS, LAND and Ping of Death attacks whether the firewall is enabled or disabled.

13.1.1 What You Can Do in the Firewall Screens

Use the **Firewall** screen (Section 13.2 on page 102) to enable firewall and/or SPI on the ZyXEL Device.

13.1.2 What You Need to Know About Firewall

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

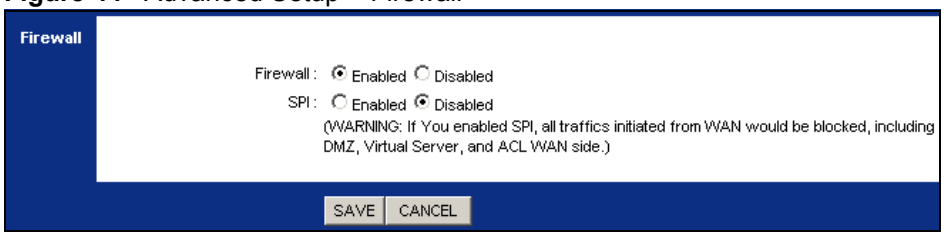
SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

13.2 The Firewall Screen

Use this screen to enable firewall and/or SPI. Click **Advanced Setup > Firewall** to display the following screen.

Figure 44 Advanced Setup > Firewall


Firewall
Firewall : Enabled Disabled
SPI : Enabled Disabled
(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)
SAVE
CANCEL

The following table describes the labels in this screen.

Table 32 Advanced > Firewall

LABEL	DESCRIPTION
Firewall	Use this field to enable or disable firewall on your ZyXEL Device.
SPI	Use this field to enable or disable SPI on your ZyXEL Device.
SAVE	Click this to save your changes.
CANCEL	Click this to restore your previously saved settings.

Enabling SPI blocks all traffic initiated from the WAN side, including the DMZ, virtual server and ACL on the WAN side.

PART VI
Access Management

Access Control (105)
Filters (109)
SNMP (115)
Universal Plug-and-Play (UPnP) (117)
Dynamic DNS Setup (129)
CWMP (131)

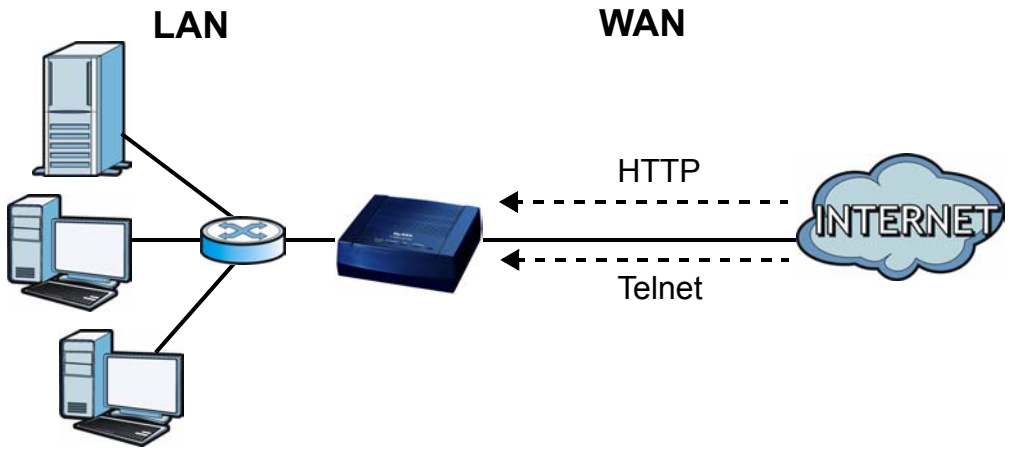
14 Access Control

14.1 Access Control Overview

Access Control allows you to determine which application can access which ZyXEL Device interface from which computers.

The following figure shows access to the ZyXEL Device from the WAN being limited to HTTP (web) and Telnet only.

Figure 45 Access Control



14.1.1 The Access Control Setup Screen

Use this screen to configure from where and how users may access the ZyXEL Device.

14.1.2 Access Control Interfaces

You may manage your ZyXEL Device via:

- **WAN**
- **LAN**
- **Both** (LAN and WAN)

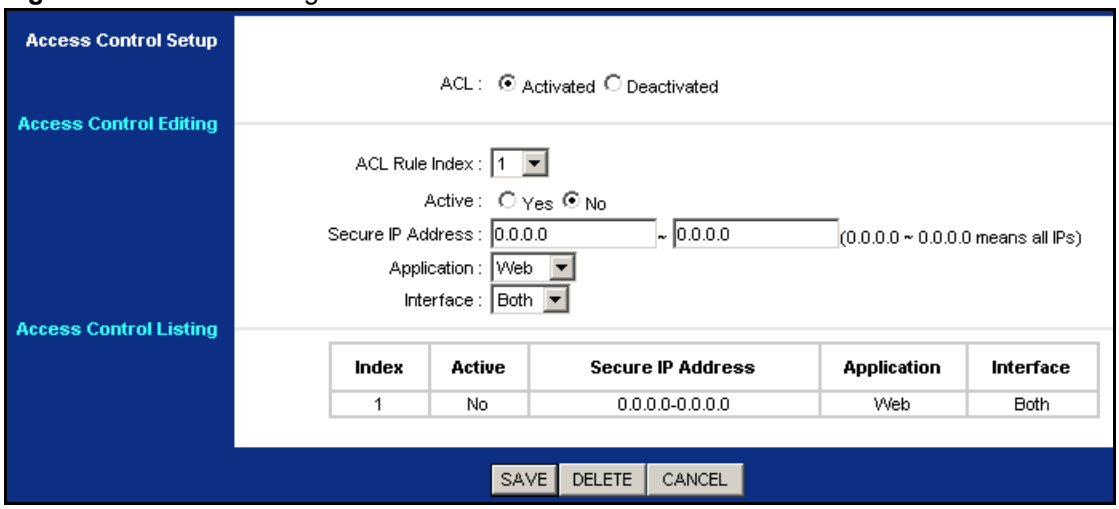
14.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

14.1.4 Configuring the Access Control Setup Screen

Click **Access Management** > **ACL** to open the following screen.

Figure 46 Access Management > ACL



The following table describes the fields in this screen.

Table 33 Access Management > ACL

LABEL	DESCRIPTION
Access Control Setup	
ACL	Select **Activated** to enable access control on the ZyXEL Device or select **Deactivated** to disable it.
Access Control Editing	
ACL Rule Index	Select an index rule number in order to edit or delete it.
Active	Select **Yes** to enable this active control rule or **No** to disable it.
Secure IP Address	Enter the range of IP addresses of computers that are allowed to access the device. 0.0.0.0 ~ 0.0.0.0 means that any computer can access the ZyXEL Device. If you want just one computer to be able to access the ZyXEL Device, then enter its IP address in both fields.
Application	Select the service through which the computer can access the device. • If you want to allow a user to connect to the ZyXEL Device using the web configurator, select **Web**. • If you want to allow a user to connect to the ZyXEL Device using Telnet, select **Telnet**. • If you want to allow a user to upload firmware to the ZyXEL Device, select **FTP**. • If you want to allow an administrator to send SNMP commands, select **SNMP**. • If you want to allow a user to find the ZyXEL Device on the network (for troubleshooting purposes, for example), select **Ping**. • Select **ALL** to allow access for all services. You cannot select a combination of services.

Table 33 Access Management > ACL (continued)

LABEL	DESCRIPTION
Interface	Select the port through which you can access the device. Select **Both** for access via either port. If you configure 0.0.0.0 ~ 0.0.0.0 **Secure IP Address**, **ALL** services and **WAN** interface, you will not be able to access the device at all from the LAN unless you configure another rule for LAN access.
Access Control Listing	The summary table displays the configured parameters for the selected rule.
SAVE	Click this so save your changes..
DELETE	Select an access control rule index number and click this to remove it.
CANCEL	Click this to restore your previously saved settings.

15 Filters

15.1 Overview

This chapter introduces three types of filters supported by the ZyXEL Device. You can configure rules to restrict traffic by IP addresses, MAC addresses, application types and/or URLs.

15.1.1 What You Can Do in the Filter Screens

- Use the **IP/MAC Filter** screen (Section 15.2 on page 110) to create IP/MAC filter rules.
- Use the **Application Filter** screen (Section 15.3 on page 112) to allow or deny traffic from certain types of applications.
- Use the **URL Filter** screen (Section 15.4 on page 113) to block access to web sites.

15.1.2 What You Need to Know About Filtering

IP/MAC Filter Structure

An IP/MAC filter set consists of one or more filter rules. The ZyXEL Device allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

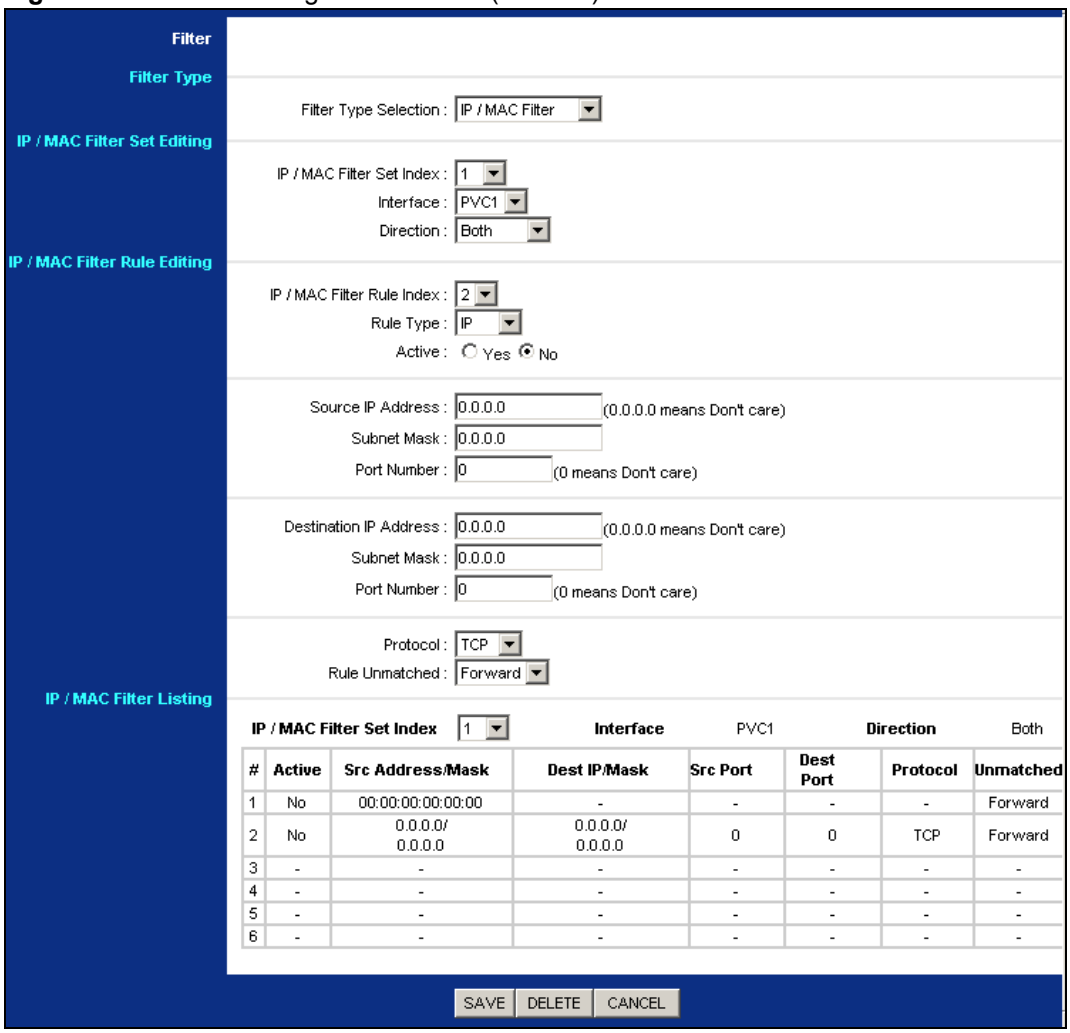
URL

The URL (Uniform Resource Locator) identifies and helps locates resources on a network. On the Internet the URL is the web address that you type in the address bar of your Internet browser, for example “http://www.zyxel.com”.

15.2 The IP/MAC Filter Screen

Use this screen to create and apply IP/MAC filters. Click **Access Management** > **Filter** and select **IP/MAC Filter** in the **Filter Type Selection** field. The screen appears as shown.

Figure 47 Access Management > Filter (IP/MAC)


Filter
Filter Type
Filter Type Selection : IP / MAC Filter
IP / MAC Filter Set Editing
IP / MAC Filter Set Index : 1
Interface : PVC1
Direction : Both
IP / MAC Filter Rule Editing
IP / MAC Filter Rule Index : 2
Rule Type : IP
Active : Yes No
Source IP Address : 0.0.0.0 (0.0.0.0 means Don't care)
Subnet Mask : 0.0.0.0
Port Number : 0 (0 means Don't care)
Destination IP Address : 0.0.0.0 (0.0.0.0 means Don't care)
Subnet Mask : 0.0.0.0
Port Number : 0 (0 means Don't care)
Protocol : TCP
Rule Unmatched : Forward
IP / MAC Filter Listing
IP / MAC Filter Set Index 1 Interface PVC1 Direction Both
Active Src Address/Mask Dest IP/Mask Src Port Dest Port Protocol Unmatched
1 No 00:00:00:00:00:00 - - - - Forward
2 No 0.0.0.0/ 0.0.0.0 0.0.0.0/ 0.0.0.0 0 0 TCP Forward
3 - - - - - - -
4 - - - - - - -
5 - - - - - - -
6 - - - - - - -
SAVE
DELETE
CANCEL

The following table describes the labels in this screen.

Table 34 Access Management > Filter (IP/MAC)

LABEL	DESCRIPTION
Filter Type	
Filter Type Selection	Select the filter type from the drop-down list box. Available options are **IP/MAC Filter**, **Application Filter** and **URL Filter**.
IP/MAC Filter Set Editing	
IP/MAC Filter Set Index	Select the index number of the filter set.
Interface	Select the PVC to which to apply the filter.
Direction	Apply the filter to **Both**, **Incoming** or **Outgoing** traffic direction.
IP/MAC Filter Rule Editing	

Table 34 Access Management > Filter (IP/MAC) (continued)

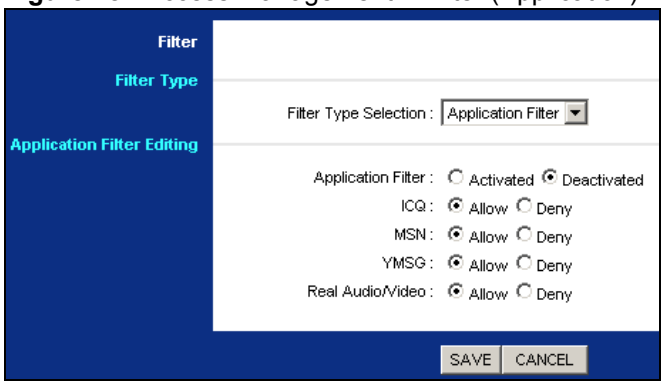
LABEL	DESCRIPTION
IP/MAC Filter Rule Index	Select the index number of the filter rule.
Rule Type	Select **IP** or **MAC** type to configure the rule. Use the **IP Filter** to block traffic by IP addresses. Use the **MAC Filter** to block traffic by MAC address.
Active	Use this field to enable or disable the rule.
Source IP Address	Enter the source IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0.
Subnet Mask	Enter the IP subnet mask for the source IP address
Port Number	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Destination IP Address	Enter the destination IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0.
Subnet Mask	Enter the IP subnet mask for the destination IP address.
Port Number	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Protocol	Select **ICMP**, **TCP** or **UDP** for the upper layer protocol.
MAC Address	This field is only available when you select **MAC** in the **Rule Type** field. Enter the MAC address of the packets you wish to filter.
Rule Unmatched	Select the action for a packet not matching the rule. Select **Forward** to forward traffic immediately and skip checking the remaining rules. Select **Next** to check the next rule.
IP/MAC Filter Listing	
IP/MAC Filter Set Index	Select the index number of the filter set from the drop-downl list box.
Interface	This is the interface that the filter set applies to.
Direction	The filter set applies to this traffic direction.
#	This is the index number of the rule in a filter set.
Active	This field shows whether the rule is activated.
Src Address/Mask	This is the source IP address and subnet mask when you select **IP** as the rule type. This is the MAC address when you select **MAC** as the rule type.
Dest IP/Mask	This is the destination IP address and subnet mask.
Src Port	This is the source port number.
Dest Port	This is the destination port number.
Protocol	This is the upper layer protocol.
Unmatched	When a packet doesn't match the rule, this is the action the ZyXEL Device takes on the packet.
SAVE	Click this to save your changes.
DELETE	Click this to remove the filter rule.
CANCEL	Click this to restore your previously saved settings.

15.3 The Application Filter Screen

Use this screen to allow or deny traffic for certain types of applications. The application filter provides a convenient way to manage the use of various applications on the network.

Click **Access Management** > **Filter** and select **Application Filter** in the **Filter Type Selection** field. The screen appears as shown.

Figure 48 Access Management > Filter (Application)



The following table describes the labels in this screen.

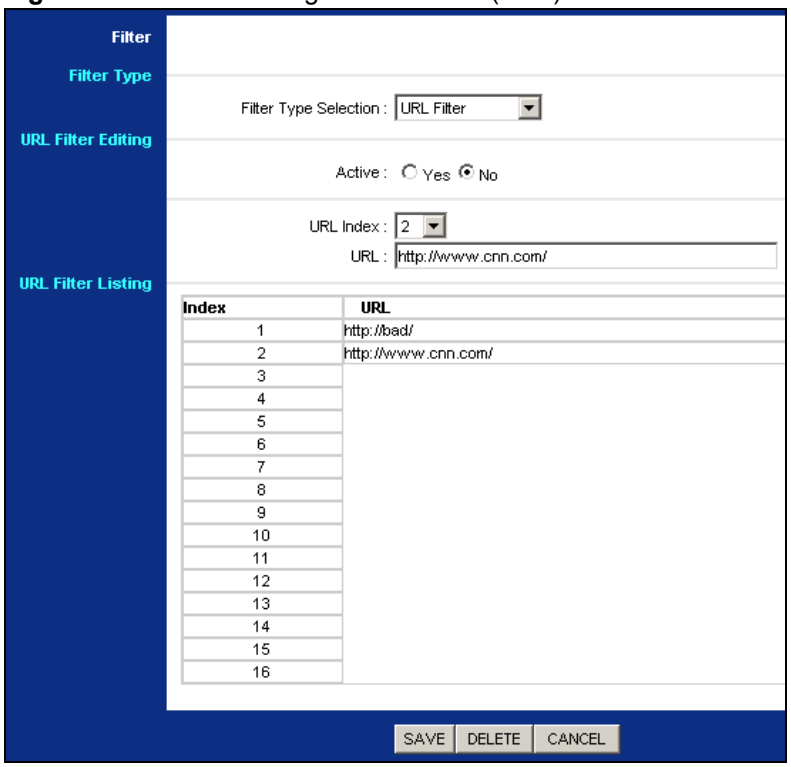
Table 35 Access Management > Filter (Application)

LABEL	DESCRIPTION
Application Filter	Use this field to enable or disable the application filter.
ICQ	Use this field to allow or deny ICQ traffic.
MSN	Use this field to allow or deny MSN traffic.
YMSG	Use this field to allow or deny Yahoo Messenger traffic
Real Audio/Video	Use this field to allow or deny transferring RealPlayer format files.
SAVE	Click this to save your changes.
CANCEL	Click this to restore your previously saved settings.

15.4 The URL Filter Screen

Use this screen to block websites by URL. Click **Access Management** > **Filter** and select **URL Filter** in the **Filter Type Selection** field.. The screen appears as shown.

Figure 49 Access Management > Filter (URL)



The following table describes the labels in this screen.

Table 36 Access Management > Filter (URL)

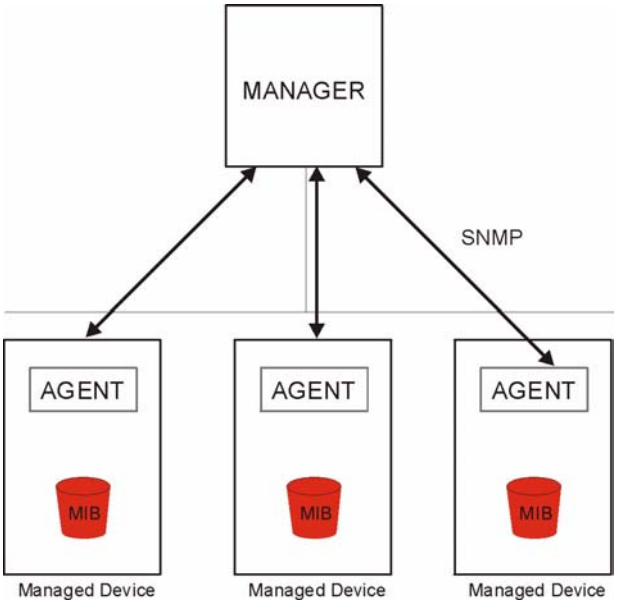
LABEL	DESCRIPTION
URL Filter Editing	
Active	Use this field to enable or disable the URL filter.
URL Index	Select the index number of the filter.
URL	Enter the URL for the ZyXEL Device to block.
URL Filter Listing	
Index	This is the index number of the filter rule.
URL	This is the URL you have configured the ZyXEL Device to block.
SAVE	Click this to save your changes.
DELETE	Click this to remove the filter rule.
CANCEL	Click this to restore your previously saved settings.

16 SNMP

16.1 Overview

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Figure 50 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- Set - Allows the manager to set values for object variables within an agent.

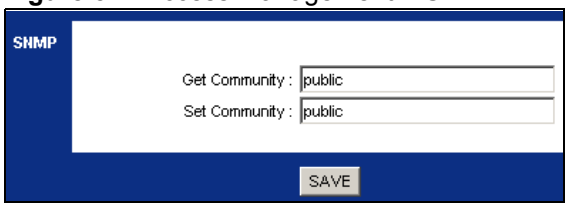
16.1.1 Supported MIBs

The ZyXEL Device supports MIB II, which is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

16.2 The SNMP Screen

Use this screen to change your ZyXEL Device's SNMP settings. Click **Access Management > SNMP** to display the following screen.

Figure 51 Access Management > SNMP



The following table describes the labels in this screen.

Table 37 Access Management > SNMP

LABEL	DESCRIPTION
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Apply	Click this to save your changes.

17

Universal Plug-and-Play (UPnP)

17.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

17.1.1 What You Can Do in the UPnP Screen

Use the **UPnP** screen (Section 17.2 on page 118) to enable UPnP on the ZyXEL Device and allow UPnP-enabled applications to automatically configure the ZyXEL Device.

17.1.2 What You Need to Know About UPnP

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

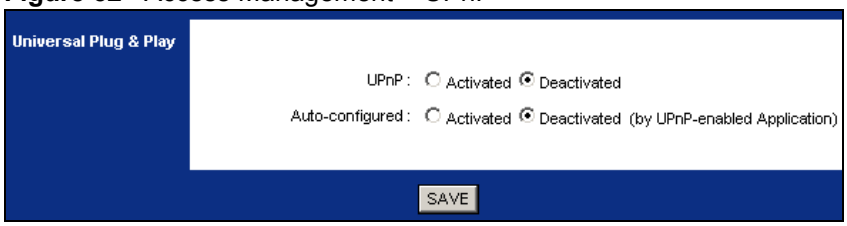
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See the following sections for examples of installing and using UPnP.

17.2 The UPnP Screen

Use the following screen to configure the UPnP settings on your ZyXEL Device. Click **Access Management > UPnP** to display the screen shown next.

Figure 52 Access Management > UPnP


Universal Plug & Play
UPnP : Activated Deactivated
Auto-configured : Activated Deactivated (by UPnP-enabled Application)
SAVE

The following table describes the fields in this screen.

Table 38 Access Management > UPnP

LABEL	DESCRIPTION
UPnP	Use this field to enable or disable UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Auto-configured	Use this field to allow or disable UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
SAVE	Click this to save your changes.

17.3 Installing UPnP in Windows Example

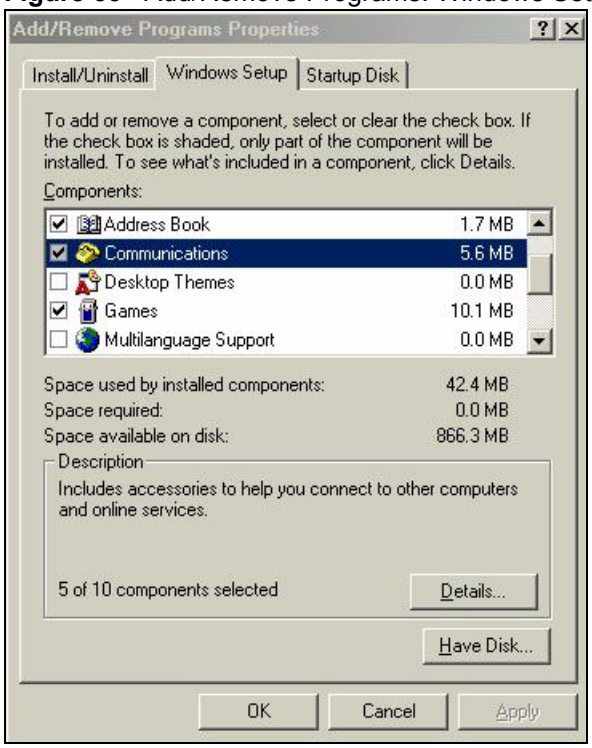
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

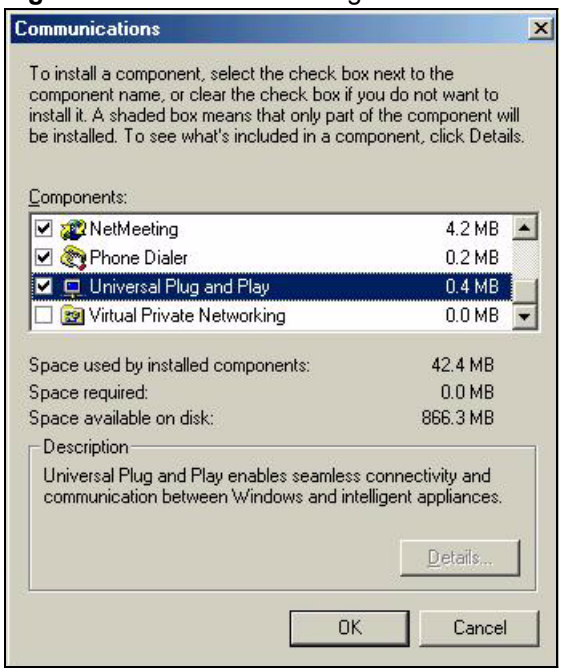
1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 53 Add/Remove Programs: Windows Setup: Communication


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 54 Add/Remove Programs: Windows Setup: Communication: Components


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

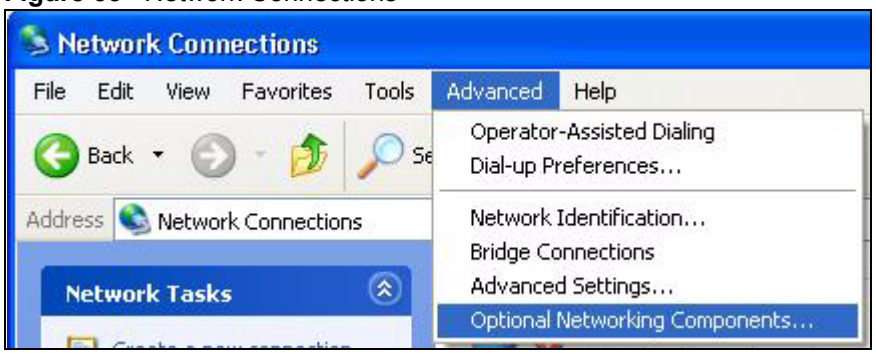
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

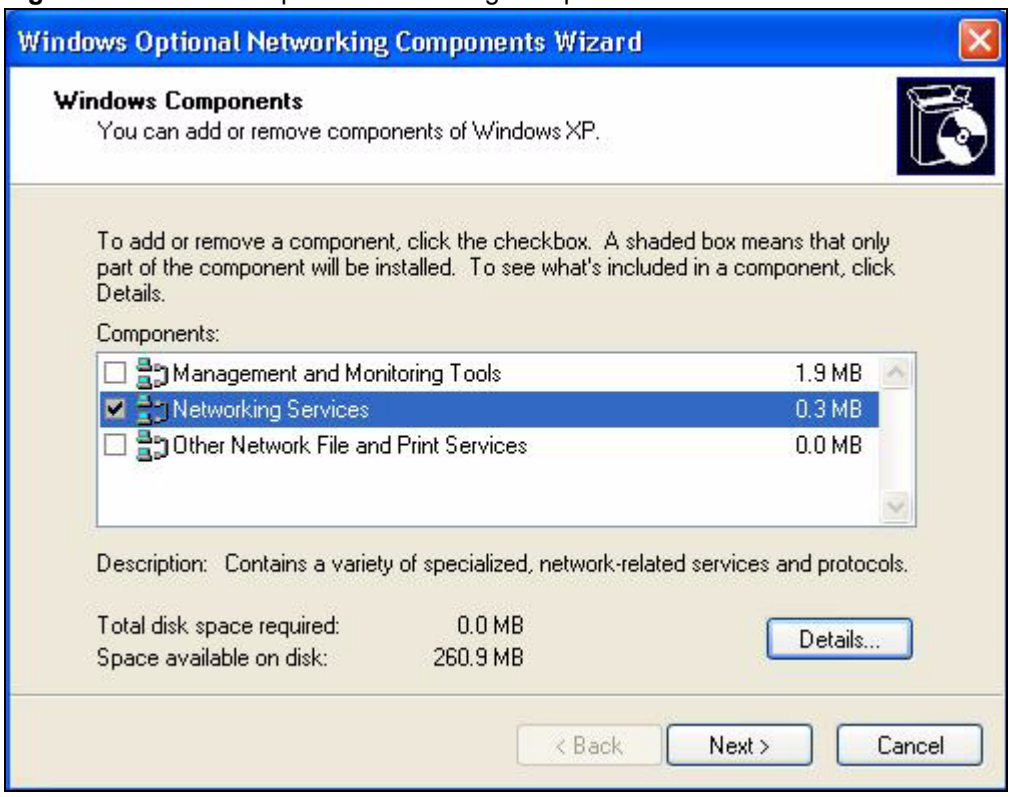
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components …**.

Figure 55 Network Connections



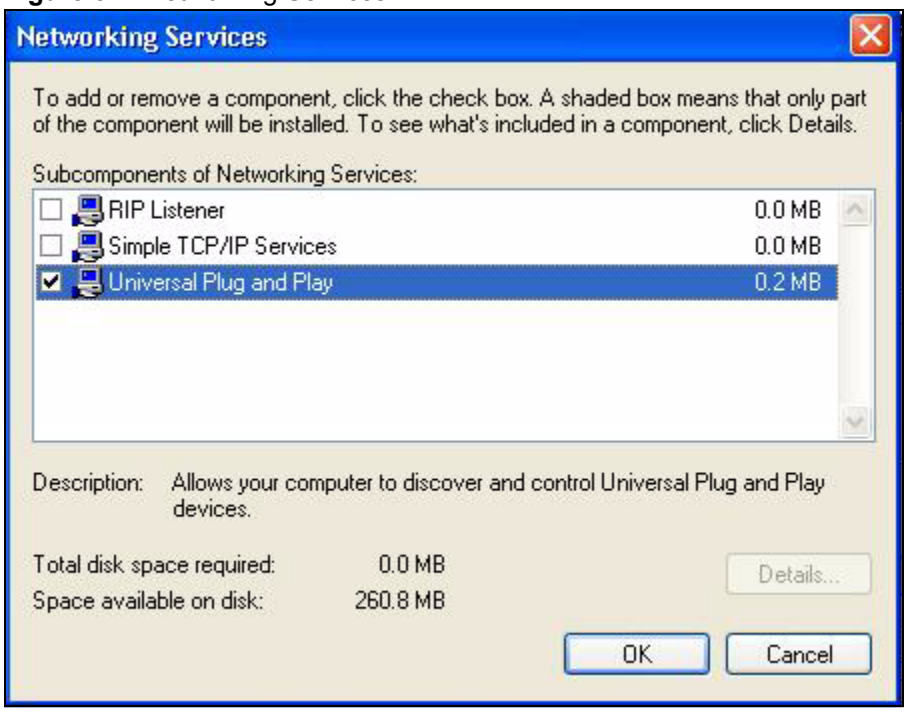
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 56 Windows Optional Networking Components Wizard


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 57 Networking Services


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

17.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 58 Network Connections

3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 59 Internet Connection Properties

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 60 Internet Connection Properties: Advanced Settings

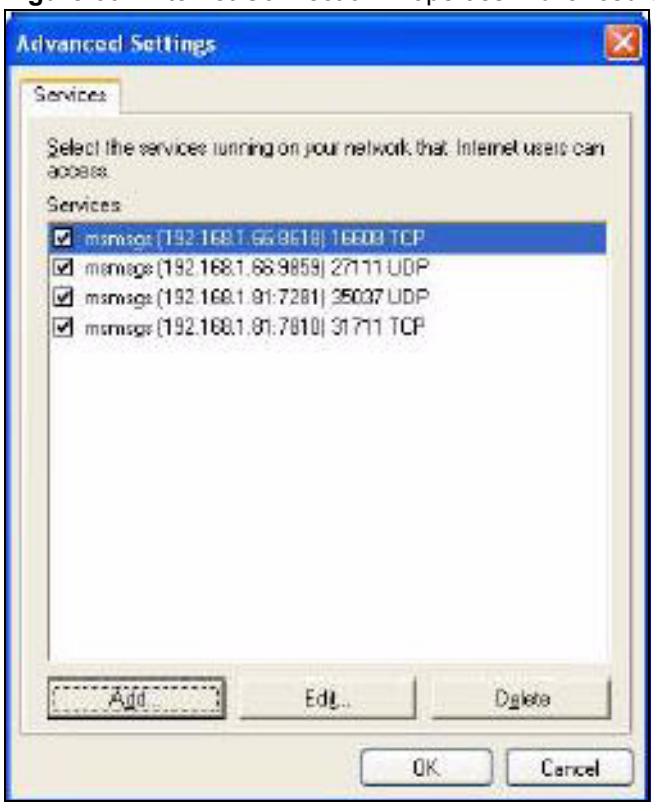
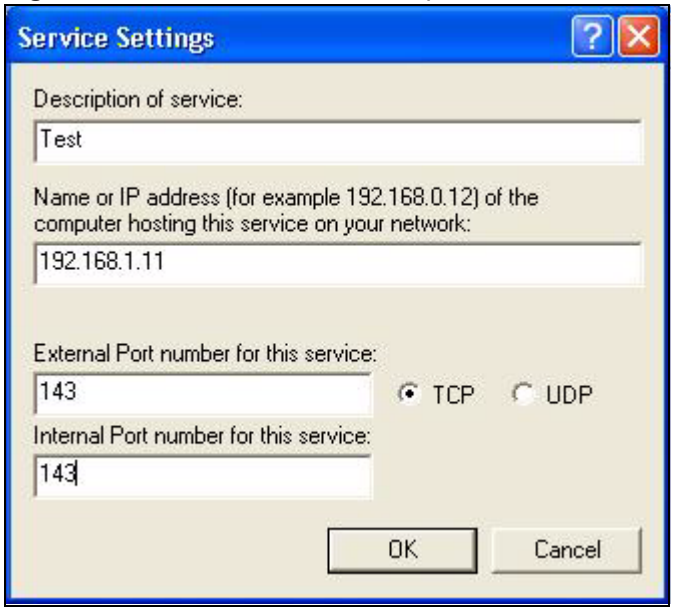


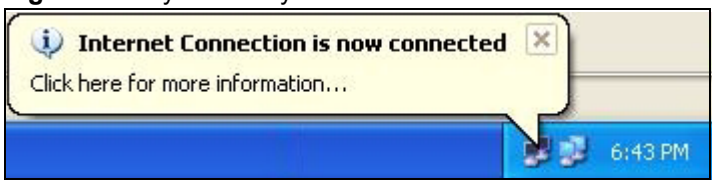
Figure 61 Internet Connection Properties: Advanced Settings: Add



5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 62 System Tray Icon



7 Double-click on the icon to display your current Internet connection status.

Figure 63 Internet Connection Status

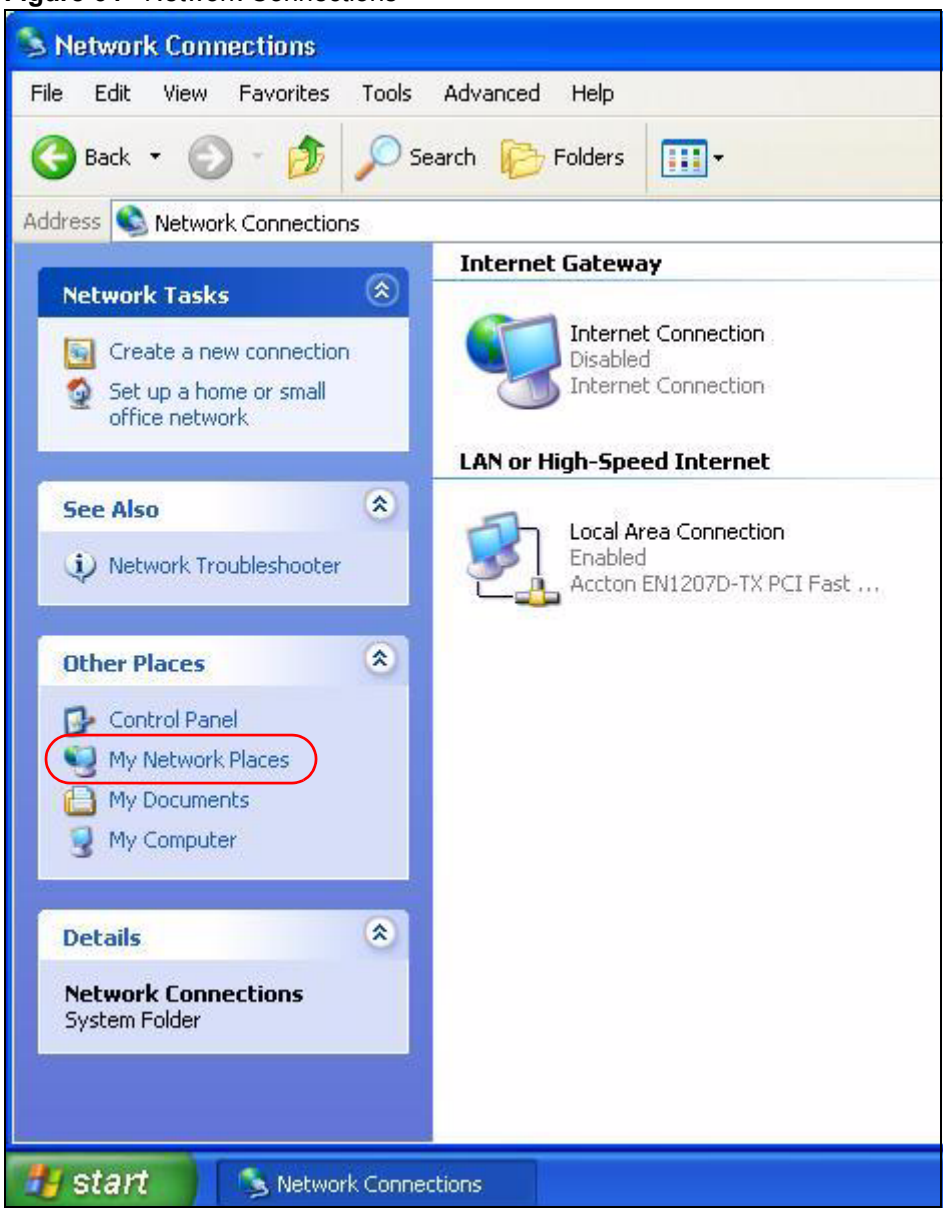
Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.
2 Double-click **Network Connections**.
3 Select **My Network Places** under **Other Places**.

Figure 64 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 65 Network Connections: My Network Places

6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

Figure 66 Network Connections: My Network Places: Properties: Example

18

Dynamic DNS Setup

18.1 Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

18.1.1 What You Can Do in the DDNS Screen

Use the **Dynamic DNS** screen (Section 18.2 on page 130) to enable DDNS and configure the DDNS settings on the ZyXEL Device.

18.1.2 What You Need To Know About DDNS

DYNDNS Wildcard

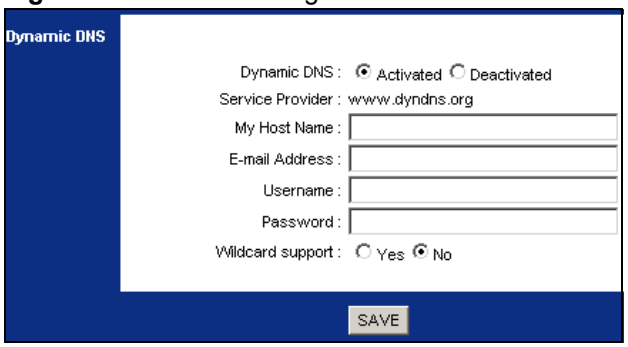
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

18.2 The Dynamic DNS Screen

Use this screen to change your ZyXEL Device's DDNS. Click **Access Management > DDNS**. The screen appears as shown.

Figure 67 Access Management > DDNS



The following table describes the fields in this screen.

Table 39 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	Use this field to enable or disable dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
My Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
Username	Type your username.
Password	Type the password assigned to you.
Wildcard support	Use this field to enable or disable DynDNS Wildcard.
SAVE	Click this to save your changes.

19

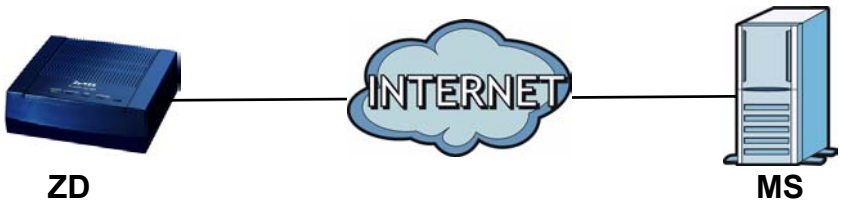
CWMP

19.1 Overview

The ZyXEL Device supports TR-069 Amendment 1 (CPE WAN Management Protocol Release 2.0) and TR-069 Amendment 2 (CPE WAN Management Protocol v1.1, Release 3.0).

TR-069 is a protocol that defines how your ZyXEL Device (**ZD**) can be managed via a management server (**MS**) such as ZyXEL's Vantage Access.

Figure 68 LAN and WAN



An administrator can use a management server to remotely set up the ZyXEL device, modify settings, perform firmware upgrades as well as monitor and diagnose the ZyXEL device.

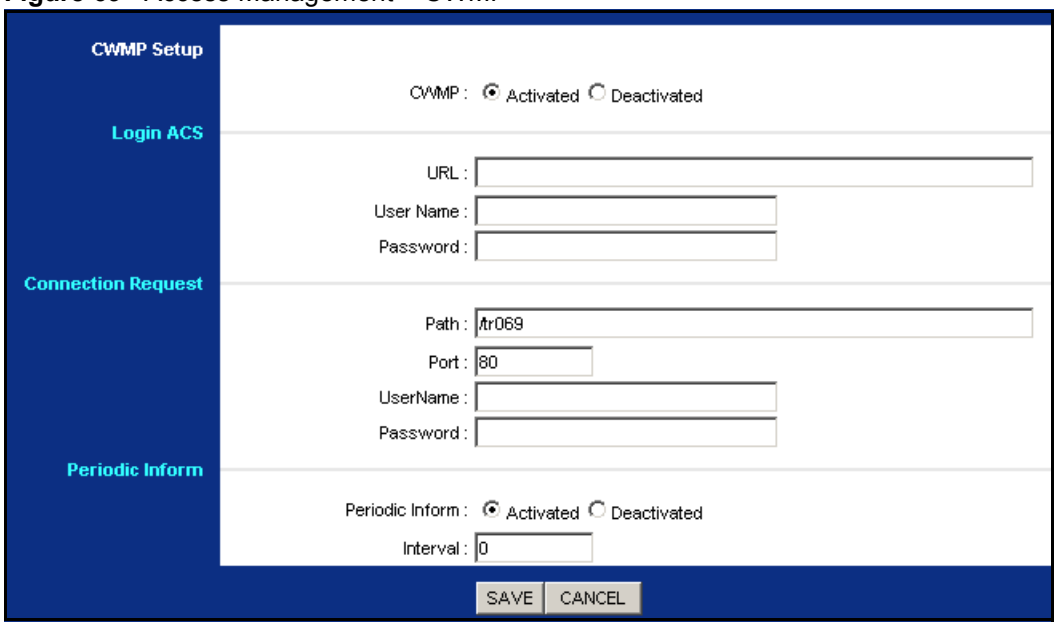
In order to use CWMP, you need to configure the following steps:

1. Activate CWMP
2. Specify the URL, username and password.
3. Activate periodic inform and specify an interval value.

19.2 The CWMP Setup Screen

Use this screen to configure your ZyXEL Device to be managed by a management server. Click **Access Management** > **CWMP** to display the following screen.

Figure 69 Access Management > CWMP



The following table describes the fields in this screen.

Table 40 Access Management > CWMP

LINK	DESCRIPTION
CWMP Setup	
CWMP	Select **Activated** to allow the ZyXEL Device to be managed by a management server or select **Deactivated** to not allow the ZyXEL Device to be managed by a management server.
Login ACS	Configure this part of the screen to log into the management server.
URL	Type the IP address or domain name of the management server. If the ZyXEL Device is behind a NAT router that assigns it a private IP address, you will have to configure a NAT port forwarding rule on the NAT router.
User Name	The user name is used to authenticate the ZyXEL Device when making a connection to the management server. This user name on the management server and the ZyXEL Device must be the same. Type a user name of up to 255 printable characters found on an English-language keyboard. Spaces and characters such as @#$%^&*()_+ are allowed.
Password	The password is used to authenticate the ZyXEL Device when making a connection to the management server. This password on the management server and the ZyXEL Device must be the same. Type a password of up to 255 printable characters found on an English-language keyboard.
Connection Request	Use this part of the screen to allow the management server to connect to the ZyXEL Device after a successful login.
Path	Type the IP address or domain name of the ZyXEL Device. The management server uses this path to verify the ZyXEL Device.

Table 40 Access Management > CWMP (continued)

LINK	DESCRIPTION
Port	The default port for access to the ZyXEL Device from the management server is the HTTP port, port 80. If you change it, make sure it does not conflict with another port on your network and it is recommended to use a port number above 1024 (not a commonly used port). The management server should use this port to connect to the ZyXEL Device. You may need to alter your NAT port forwarding rules if they were already configured.
UserName	The user name is used to authenticate the management server when connecting to the ZyXEL Device. Type a user name of up to 255 printable characters found on an English-language keyboard. Spaces and characters such as @#$%^&*()_+ are allowed.
Password	The password is used to authenticate the management server when connecting to the ZyXEL Device. Type a password of up to 255 printable characters found on an English-language keyboard. Spaces are not allowed.
Periodic Inform	Select **Activated** to have the ZyXEL Device periodically send information to the management server (recommended if CWMP is enabled) or select **Deactivated** to not have the ZyXEL Device periodically send information to the management server
Interval	The interval is the duration in seconds for which the ZyXEL Device must attempt to connect with the management server to send information and check for configuration updates. Enter a value between 1 and 86400 seconds.
SAVE	Click this to save your changes.
CANCEL	Click this to restore your previously saved settings.

PART VII
Maintenance

Administrator Settings (137)
Time Zone (139)
Firmware (141)
System Restart (149)
Diagnostic (151)

20

Administrator Settings

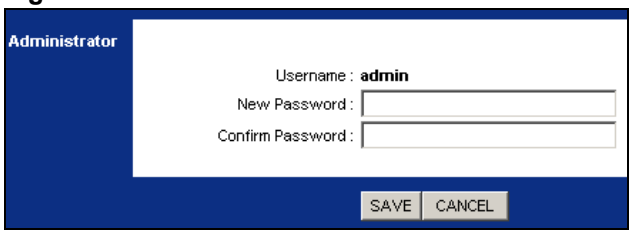
20.1 Overview

This chapter shows you how to change the system password.

20.2 The Administrator Screen

Use this screen to set a new password for your ZyXEL Device. Click **Maintenance** > **Administraton** to open the following screen.

Figure 70 Maintenance > Administraton



The following table describes the labels in this screen.

Table 41 Maintenance > Administraton

LABEL	DESCRIPTION
New Password	Type your new password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Confirm Password	Type the new password again for confirmation.
SAVE	Click this to save your changes.
CANCEL	Click this to restore your previously saved settings.

21 Time Zone

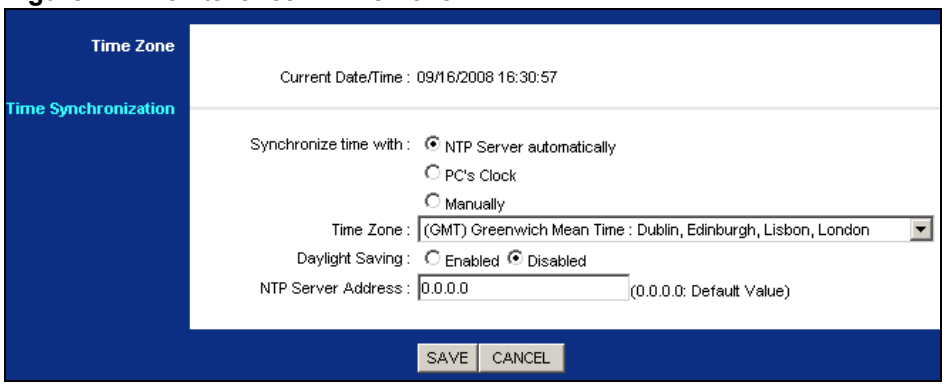
21.1 Overview

This chapter contains information about configuring your ZyXEL Device's time settings.

21.2 The Time Zone Screen

Use this screen to configure the ZyXEL Device's time based on your local time zone. To change your ZyXEL Device's time and date, click **Maintenance > Time Zone**. The screen appears as shown.

Figure 71 Maintenance > Time Zone



The following table describes the fields in this screen.

Table 42 Maintenance > Time Zone

LABEL	DESCRIPTION
Time Zone	
Current Date/Time	This field displays the date and time of your ZyXEL Device.
Time Synchronization	
Synchronize time with	Select **NTP Server automatically** to have the ZyXEL Device get the time and date from the time server. The NTP server displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. Select **PC's Clock** to have the ZyXEL Device synchronize the time with your PC. Select **Manually** to enter the time and date manually.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Table 42 Maintenance > Time Zone (continued)

LABEL	DESCRIPTION
Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select **Enabled** if you use Daylight Saving Time.
NTP Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Date	This field is only available when you want to set the time and date manually. Enter the date in this field.
Time	This field is only available when you want to set the time and date manually. Enter the time in this field.
SAVE	Click this to save your changes.
CANCEL	Click this to restore your previously saved settings.

22 Firmware

22.1 Overview

This chapter explains how to upload new firmware and manage configuration files.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.

22.1.1 What You Need To Know About Firmware

Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. Find this firmware at www.zyxel.com. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "`config.cfg`".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

Table 43 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyXEL Device.	*.bin

FTP Restrictions

FTP will not work when:

1. You have disabled the FTP service in the **Remote Management** screen.
2. The IP you entered in the Secured Client IP field does not match the client IP. If it does not match, the device will disallow the FTP session.

22.1.2 Before You Begin

Make sure the FTP service has not been disabled in the Remote Management screen.

22.1.3 Firmware and Configuration Files Examples

This section contains examples about managing configuration files and uploading firmware to your ZyXEL Device.

Using FTP to Restore Configuration

This example shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.

Restore Using FTP Session Example

Figure 72 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 22.1.1 on page 141 to read about configurations that disallow TFTP and FTP over WAN.

FTP and TFTP Firmware and Configuration File Uploads

These examples show you how to upload firmware and configuration files.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

7 Enter “quit” to exit the ftp prompt.

FTP Session Example of Firmware File Upload

Figure 73 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed in this chapter.

Refer to Section 22.1.1 on page 141 to read about configurations that disallow TFTP and FTP over WAN.

TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the device's IP address, "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Using the FTP Commands to Back Up Configuration

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your ZyXEL Device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "`bin`" to set transfer mode to binary.
6. Use "`get`" to transfer files from the ZyXEL Device to the computer, for example, "`get rom-0 config.rom`" transfers the configuration file on the ZyXEL Device to your computer and renames it "`config.rom`". See earlier in this chapter for more information on filename conventions.
7. Enter "`quit`" to exit the ftp prompt.

FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device's configuration onto your computer.

Figure 74 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 44 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.

Table 44 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

22.2 The Firmware Screen

Use this screen to manage configuration files and upload firmware to your ZyXEL Device.

Firmware Upgrade

Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 22.1.3 on page 142 for upgrading firmware using FTP/TFTP commands.

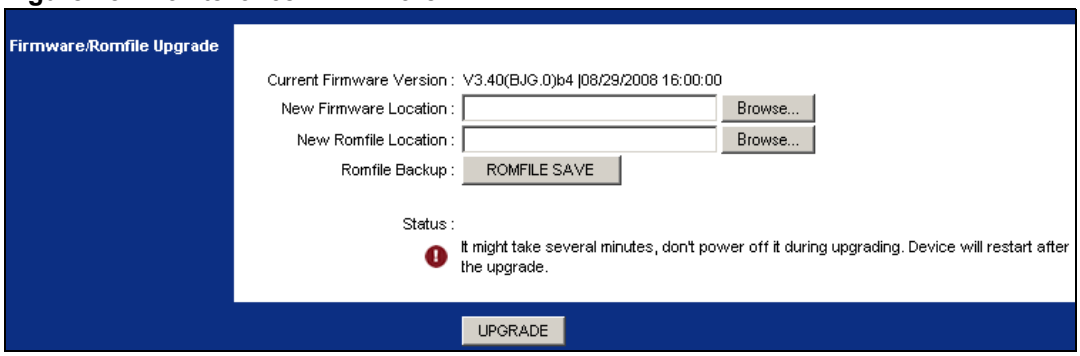
Do NOT turn off the ZyXEL Device while firmware upload is in progress!

Romfile Backup

Romfile backup allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Maintenance > Firmware** to open the following screen.

Figure 75 Maintenance > Firmware


Firmware/Romfile Upgrade
Current Firmware Version : V3.40(BJG.0)b4 |08/29/2008 16:00:00
New Firmware Location :
Browse...
New Romfile Location :
Browse...
Romfile Backup :
ROMFILE SAVE
Status :
It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.
UPGRADE

The following table describes the labels in this screen.

Table 45 Maintenance > Firmware

LABEL	DESCRIPTION
Current Firmware Version	This is the present firmware version and the date created.
New Firmware Location	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
New Romfile Location	This allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device. Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Romfile Backup	Click this to save the ZyXEL Device's current configuration to your computer.
UPGRADE	Click this to begin the upload process.

23

System Restart

23.1 Overview

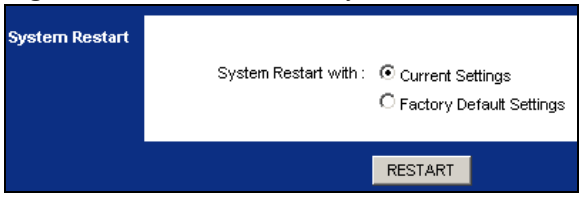
This chapter shows you how to restart your ZyXEL Device.

23.2 The System Restart Screen

System restart allows you to reboot the ZyXEL Device remotely without turning the power off. You may need to do this if the ZyXEL Device hangs, for example.

Click **Maintenance** > **SysRestart** to open the following screen.

Figure 76 Maintenance > System Restart



The following table describes the labels in this screen.

Table 46 Maintenance > System Restart

LABEL	DESCRIPTION
System Restart with	Select **Current Settings** to keep your configuration settings after the ZyXEL Device reboots. This does not affect the ZyXEL Device's configuration. Select **Factory Default Settings** to clear all user-defined configuration information and return the ZyXEL Device to its factory defaults.
RESTART	Click this to reboot the ZyXEL Device.

24

Diagnostic

24.1 Overview

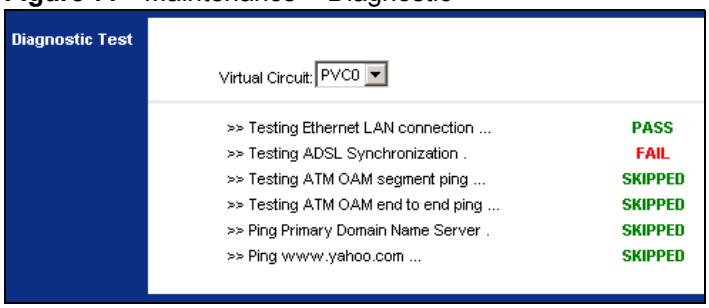
These read-only screens display information to help you identify problems with the ZyXEL Device.

24.2 The Diagnostic Screen

Use this screen to test your connection and ping an IP address. Select the virtual circuit you want to check from the drop-down list box.

Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 77 Maintenance > Diagnostic


Diagnostic Test
Virtual Circuit: PVC0
>> Testing Ethernet LAN connection ... PASS
>> Testing ADSL Synchronization . FAIL
>> Testing ATM OAM segment ping ... SKIPPED
>> Testing ATM OAM end to end ping ... SKIPPED
>> Ping Primary Domain Name Server . SKIPPED
>> Ping www.yahoo.com ... SKIPPED

PART VIII
Troubleshooting and Product Specifications

Troubleshooting (155)
Product Specifications (159)

25

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access

25.1 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure the ZyXEL Device is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
3. Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 29.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

25.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1. The default IP address is **192.168.1.1**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 30.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 30.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address (Section 8.2 on page 68), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 189.
4. If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix A on page 167. Your ZyXEL Device is a DHCP server by default.
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device. See Appendix A on page 167.
5. Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 1.6 on page 30.
6. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1. Make sure you have entered the password correctly. The default password is **1234**. The field is case-sensitive, so make sure [Caps Lock] is not on.
2. You cannot log in to the web configurator while someone is using Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.
3. Turn the ZyXEL Device off and on.
4. If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 30.

I cannot Telnet to the ZyXEL Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

25.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 29.

2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 29.
2 Turn the ZyXEL Device off and on.
3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 29. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2 Check the signal strength. If the signal strength is low, try moving your computer closer to the ZyXEL Device if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3 Turn the ZyXEL Device off and on.
4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

26

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

26.1 Hardware Specifications

Table 47 Hardware Specifications

Dimensions	(110 W) x (107 D) x (36 H) mm
Weight	165 g
Power Specification	12V DC 1A SOCB
LAN Ethernet Port	1 auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
ADSL Port	1 RJ-11 FXS POTS port
RESET Button	Restores factory defaults
Operation Temperature	0º C ~ 40º C
Storage Temperature	-20º ~ 60º C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH

26.2 Firmware Specifications

Table 48 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Username	admin
Default Password	1234
DHCP Server IP Pool	192.168.1.32 to 192.168.1.64
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!

Table 48 Firmware Specifications (continued)

Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN.
IP/MAC Address Filters	Your device's packet filtering function allows added network security and management.
Application Filter	Application filter allows you to block instant messaging programs.
URL Filter	URL filter allows you to block access to Internet web sites that contain key words (that you specify) in the URL.
QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 8 Permanent Virtual Circuits (PVCs).

Table 48 Firmware Specifications (continued)

ADSL Standards	ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G.992.2) ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM AAL5 (RFC2364) PPP over Ethernet for DSL connection (RFC2516) VC-based and LLC-based multiplexing I.610 F4/F5 OAM Annex A/B/I/J/L/M TR-067/TR-100
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol IP routing Transparent bridging for unsupported network layer protocols RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1, v2 and v3 IGMP Proxy
Management	Embedded Web Configurator CLI (Command Line Interpreter) SNMP v1 & v2c with MIB II Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore Telnet for remote management Remote Management Control: Telnet, FTP, Web, SNMP and DNS. Remote Firmware Upgrade Syslog TR-069 F4/F5 OAM

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 49 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5

Table 49 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC 2766	Network Address Translation - Protocol
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
MBM v2	Media Bandwidth Management v2
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
TR-069	TR-069 DSL Forum Standard for CPE Wan Management.
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)

26.3 Power Adaptor Specifications

Table 50 ZyXEL Device Series Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	12V 1A SOCB PA
Input Power	AC 120Volts/60Hz
Output Power	DC 12Volts/1.0A
Power Consumption	7.7 Watt max
Safety Standards	ANSI/UL 60950-1, CSA 60950-1
EUROPEAN PLUG STANDARDS	

Table 50 ZyXEL Device Series Power Adaptor Specifications (continued)

AC Power Adapter Model	
Input Power	AC 230Volts/50Hz
Output Power	DC 12Volts/1.0A
Power Consumption	8.3 Watt max
Safety Standards	CE, GS or TUV, EN60950-1

PART IX Appendices and Index

The appendices provide general information. Some details may not apply to your Product Name [short].

Setting up Your Computer's IP Address (167)

Pop-up Windows, JavaScripts and Java Permissions (189)

IP Addresses and Subnetting (197)

Services (205)

Legal Information (209)

Customer Support (213)

Index (219)

A

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

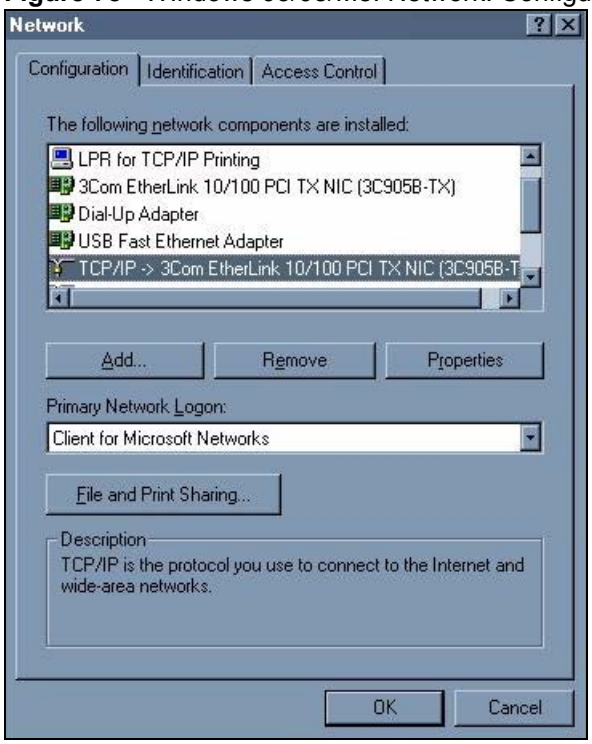
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 78 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

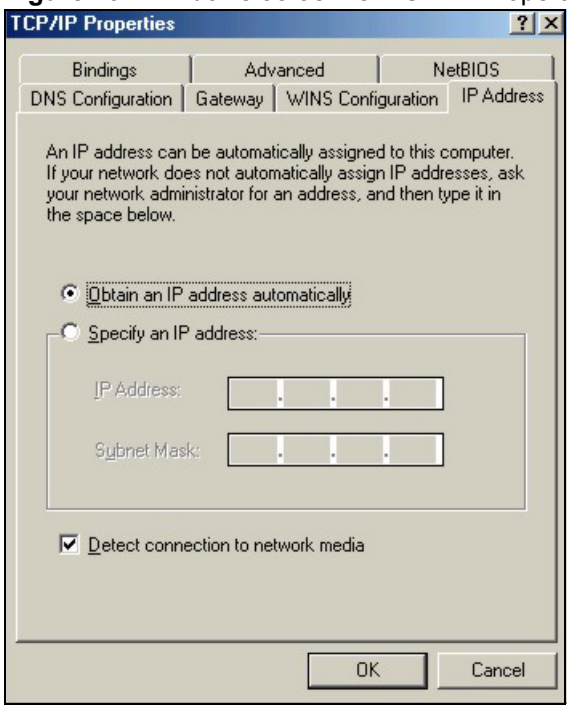
If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

Configuring

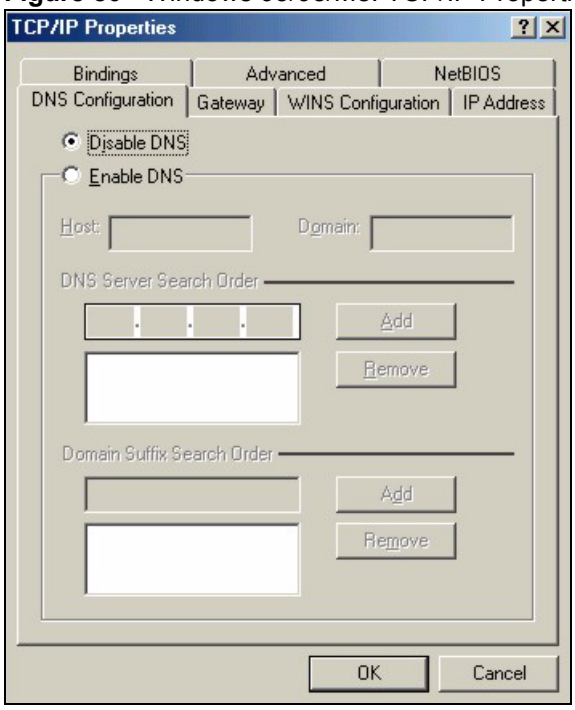
1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
2. Click the **IP Address** tab.
   - If your IP address is dynamic, select **Obtain an IP address automatically**.
   - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 79 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3. Click the **DNS** Configuration tab.
   - If you do not know your DNS information, select **Disable DNS**.
   - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 80 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your ZyXEL Device and restart your computer when prompted.

Verifying Settings

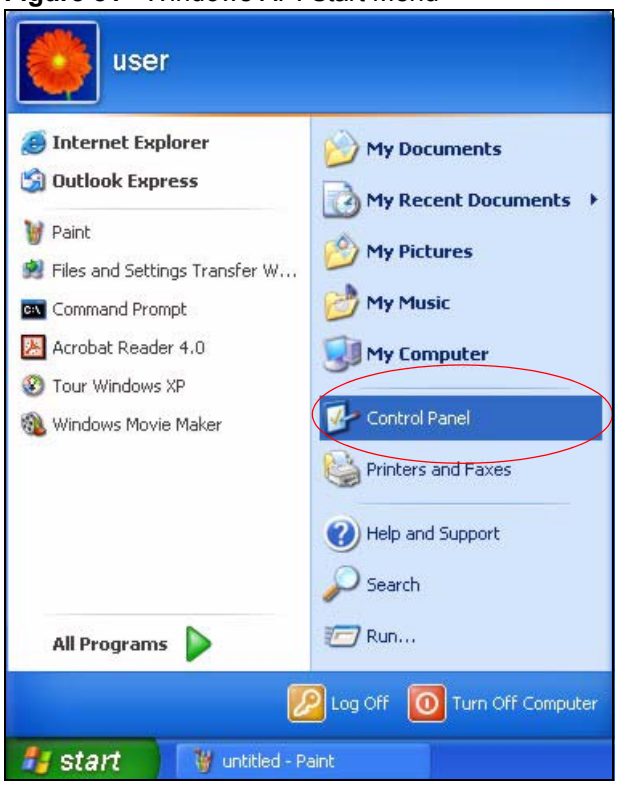
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 81 Windows XP: Start Menu

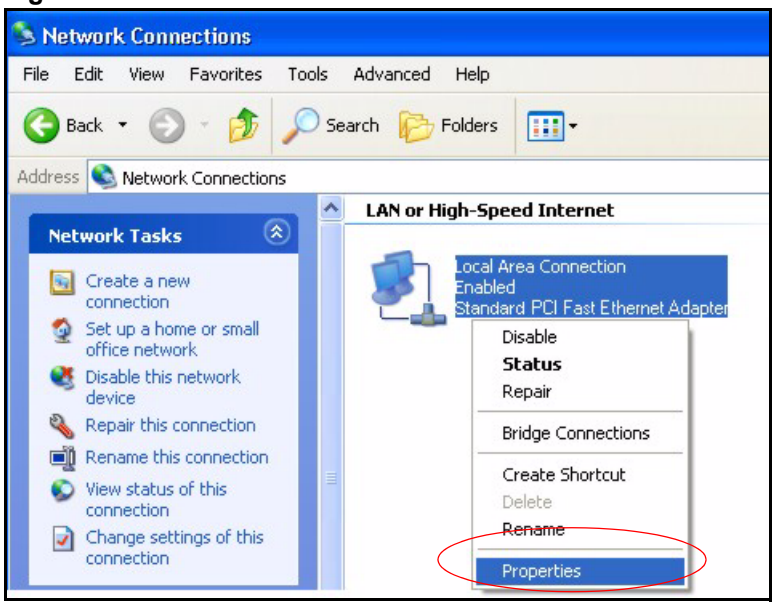


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 82 Windows XP: Control Panel

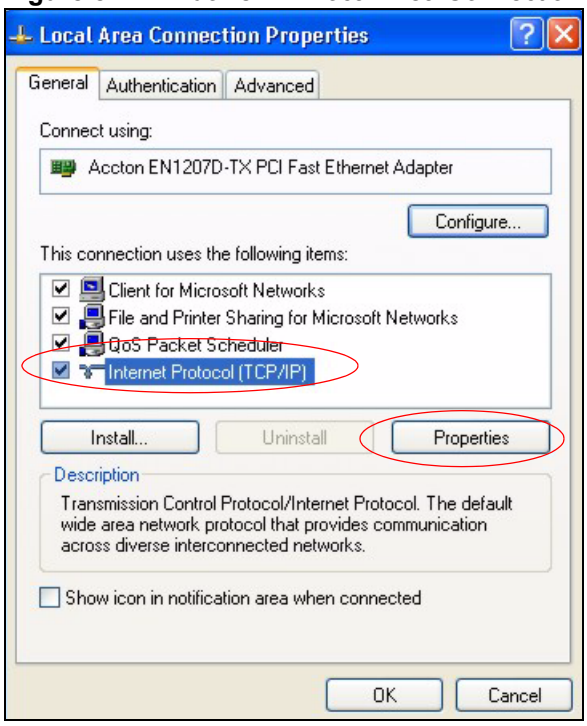
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 83 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

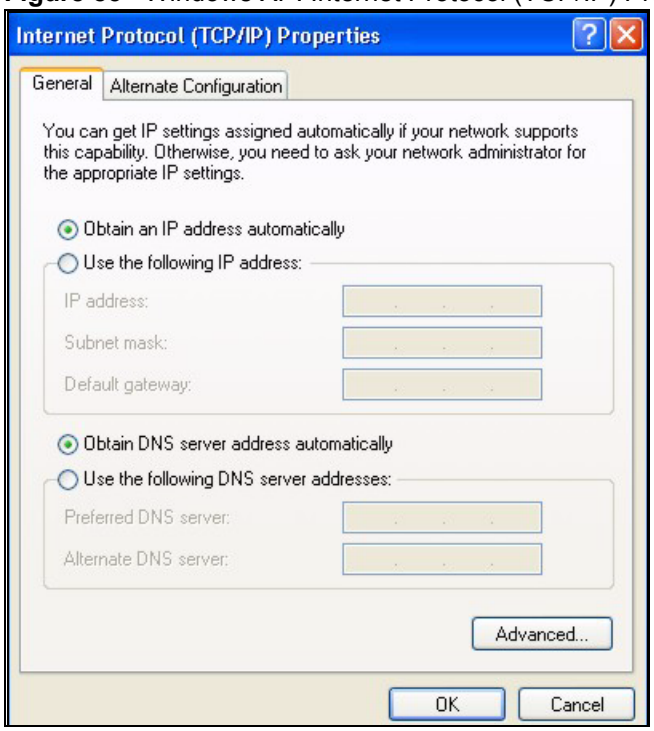
Figure 84 Windows XP: Local Area Connection Properties


Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 85 Windows XP: Internet Protocol (TCP/IP) Properties

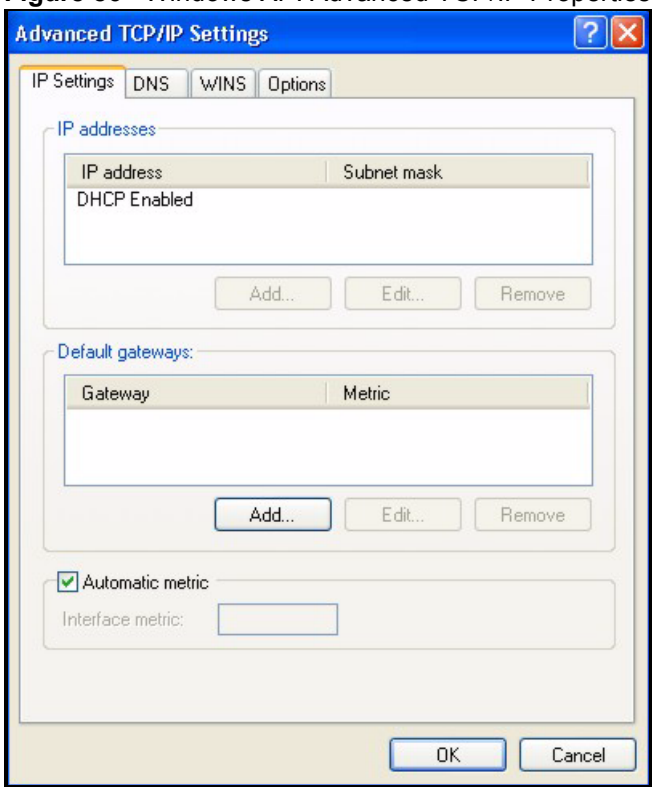

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 86 Windows XP: Advanced TCP/IP Properties

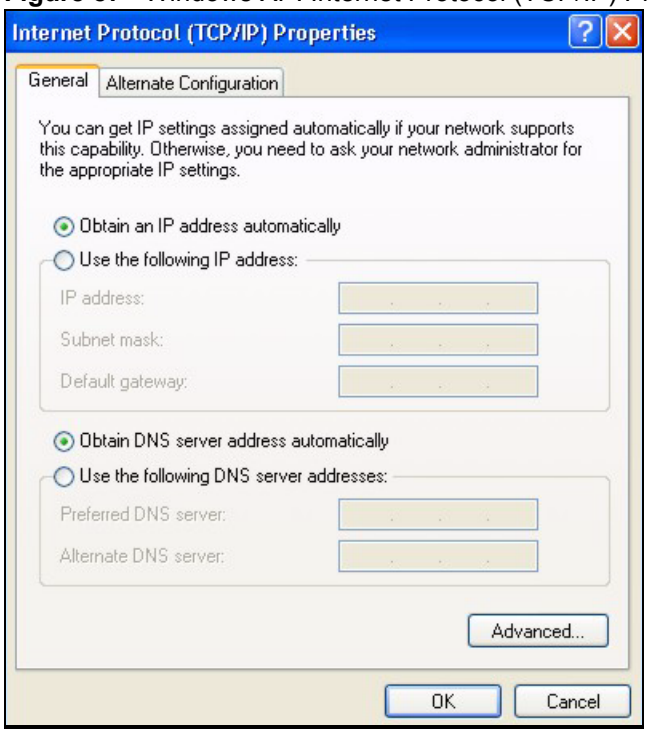


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 87 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

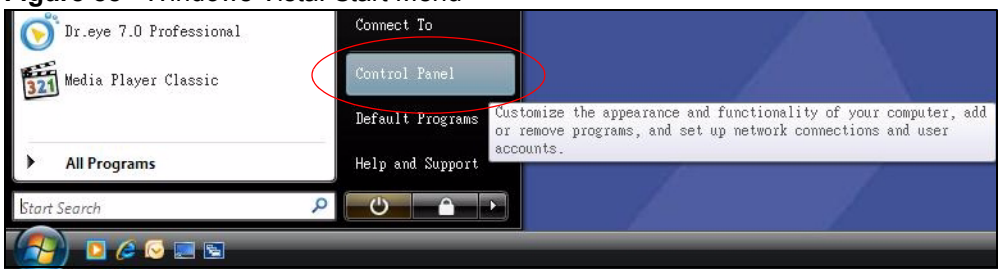
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

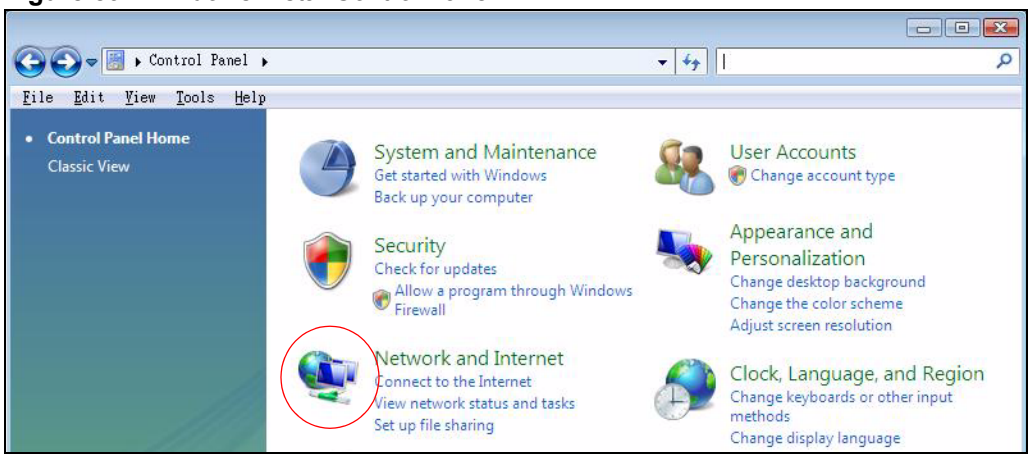
1 Click the **Start** icon, **Control Panel**.

Figure 88 Windows Vista: Start Menu


Dr.eye 7.0 Professional
Media Player Classic
All Programs
Start Search
Connect To
Control Panel
Default Programs
Help and Support
Customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

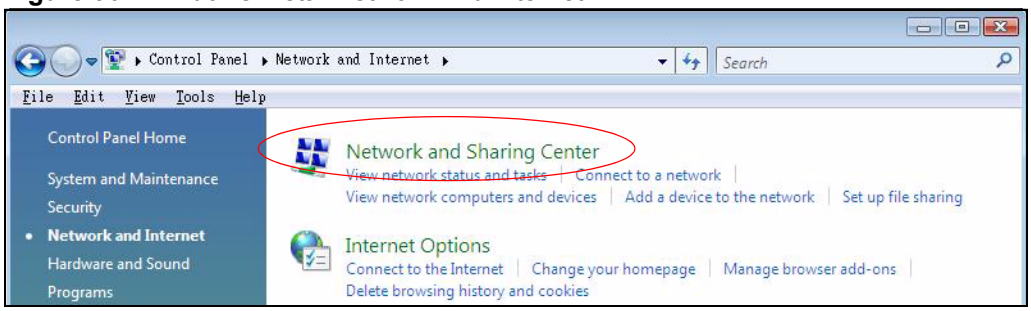
2 In the **Control Panel**, double-click **Network and Internet**.

Figure 89 Windows Vista: Control Panel



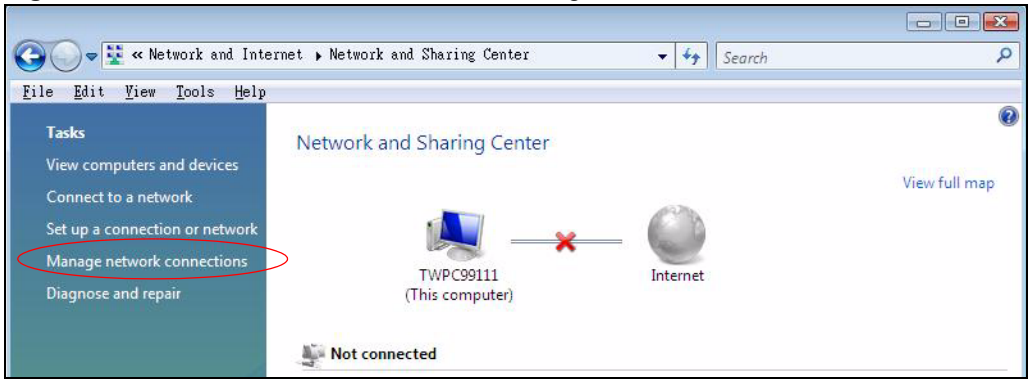
3 Click **Network and Sharing Center**.

Figure 90 Windows Vista: Network And Internet



4 Click **Manage network connections**.

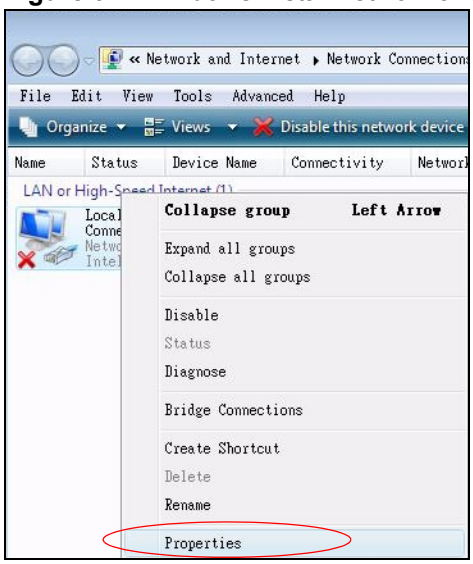
Figure 91 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then click **Properties**.

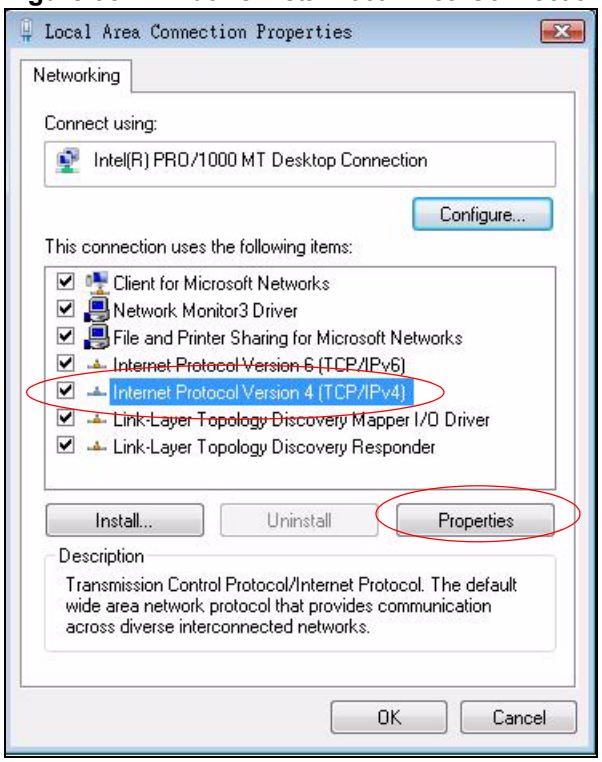
During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

Figure 92 Windows Vista: Network and Sharing Center



6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

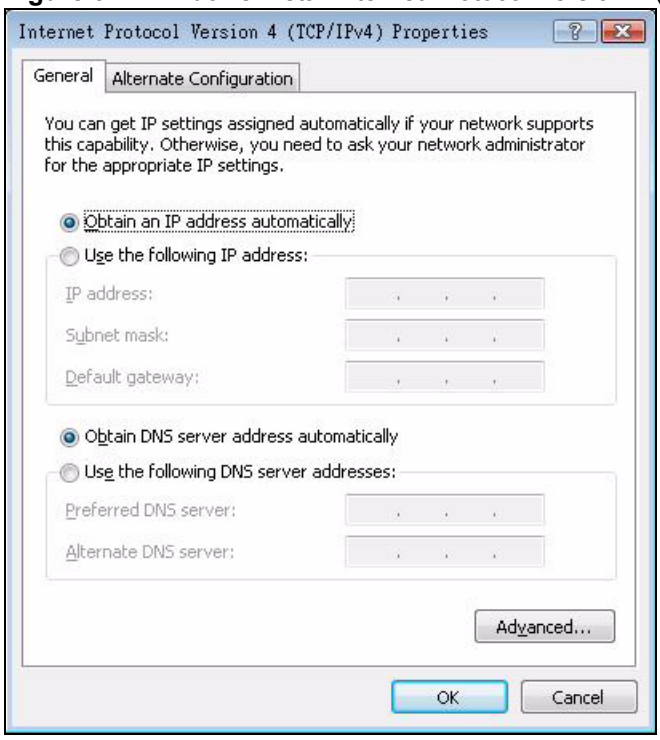
Figure 93 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 94 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties

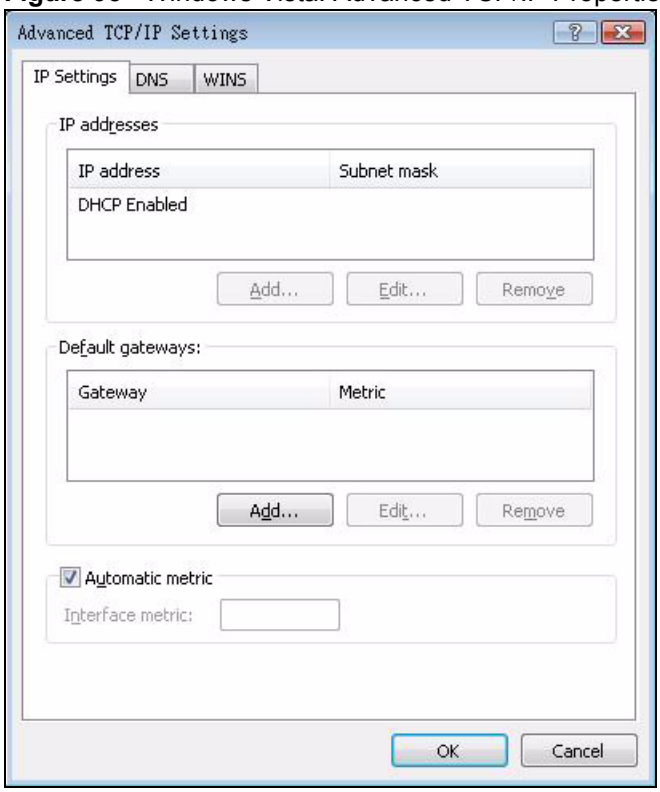

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 95 Windows Vista: Advanced TCP/IP Properties

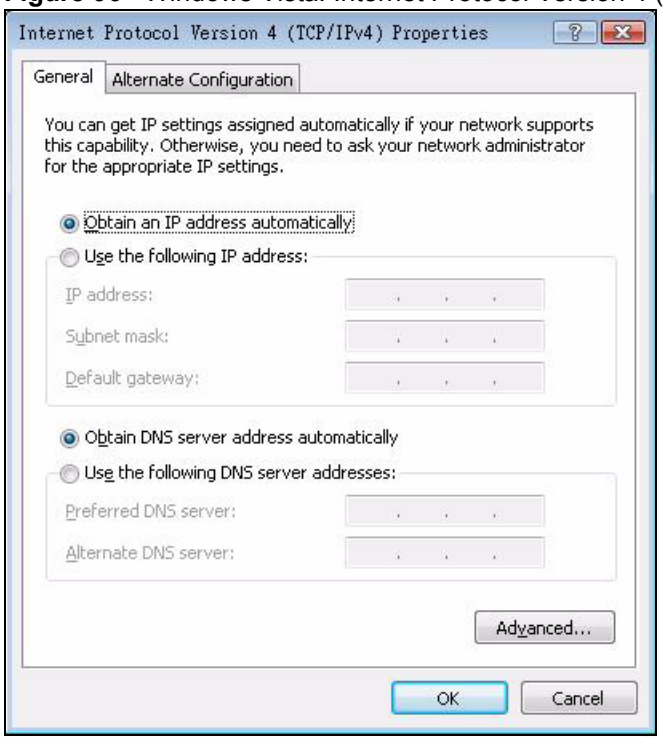


9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 96 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

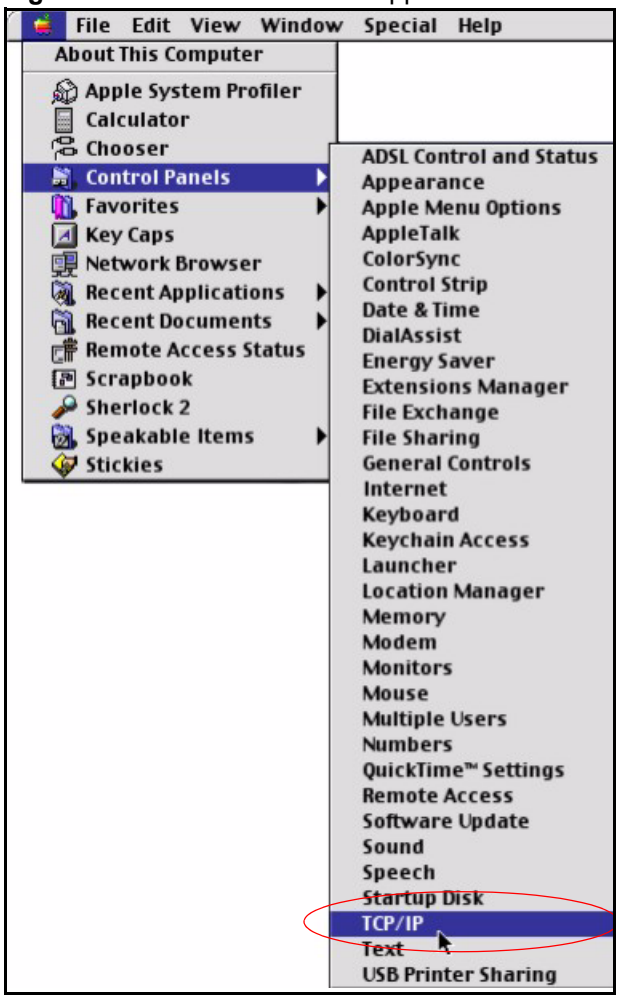
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

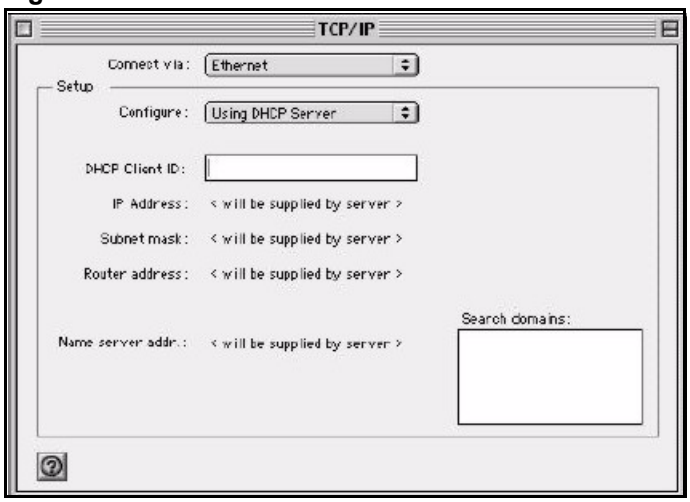
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 97 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 98 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL Device and restart your computer (if prompted).

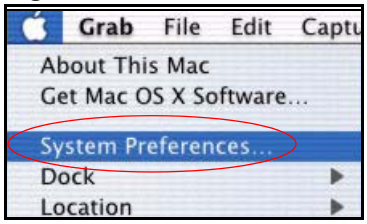
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 99 Macintosh OS X: Apple Menu

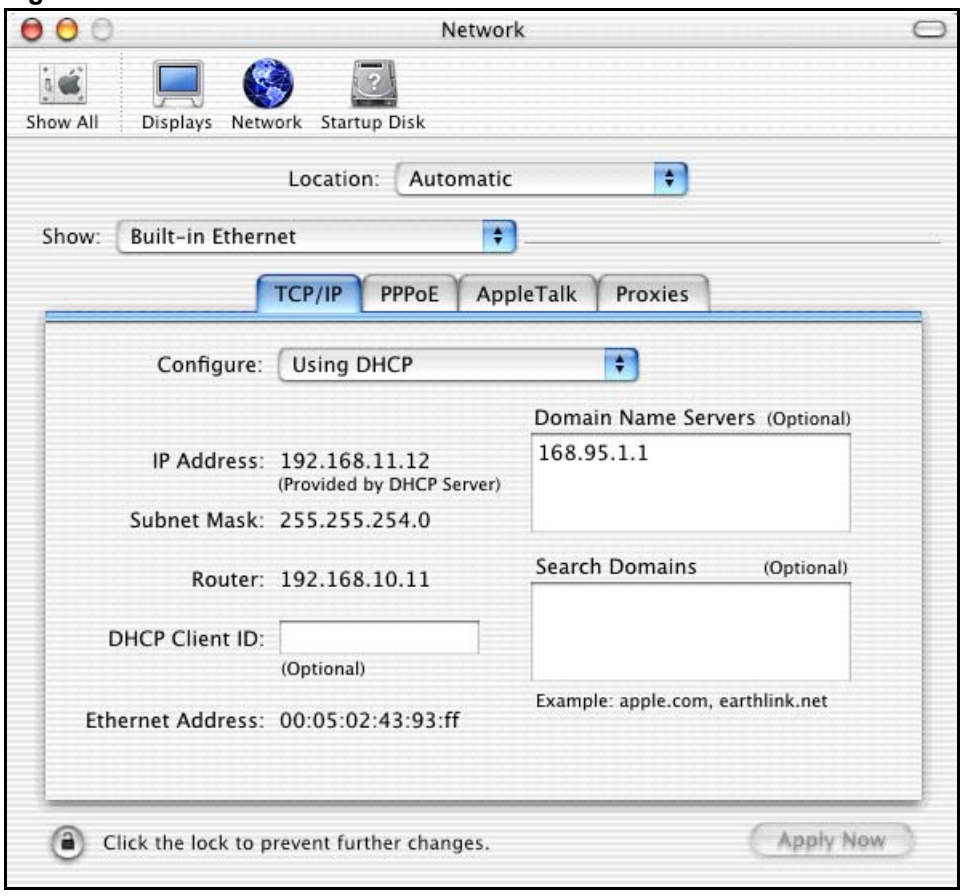


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 100 Macintosh OS X: Network



4 For statically assigned settings, do the following:
   - From the **Configure** box, select **Manually**.
   - Type your IP address in the **IP Address** box.
   - Type your subnet mask in the **Subnet mask** box.
   - Type the IP address of your ZyXEL Device in the **Router address** box.
5 Click **Apply Now** and close the window.
6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

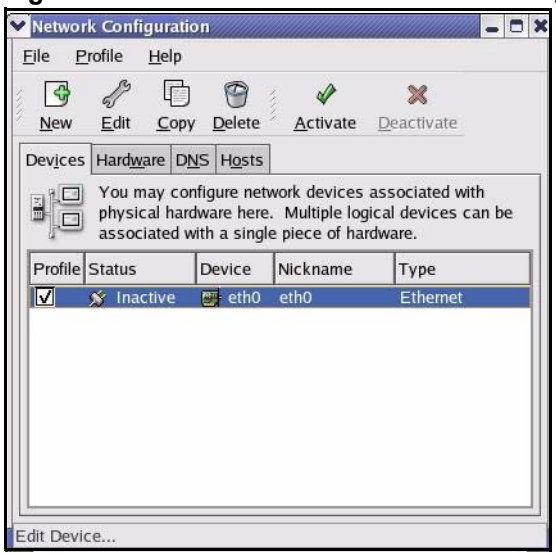
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 101 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

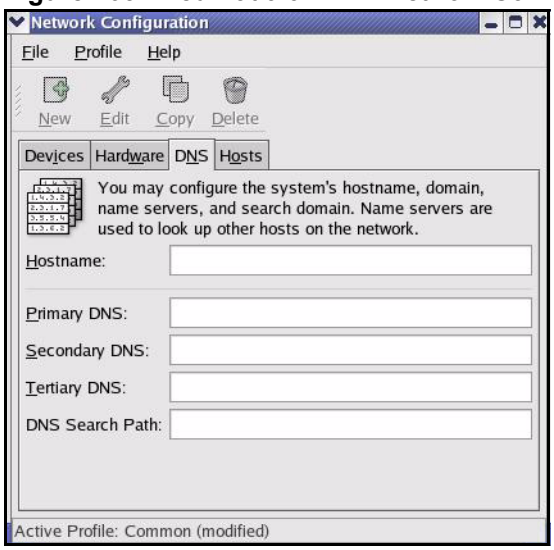
Figure 102 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 103 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 104 Red Hat 9.0: KDE: Network Configuration: Activate

Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 105 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 106 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 107 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 108 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 109 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

B

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

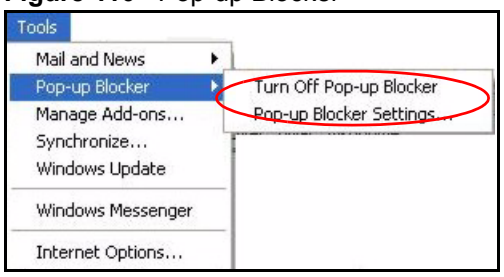
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 110 Pop-up Blocker

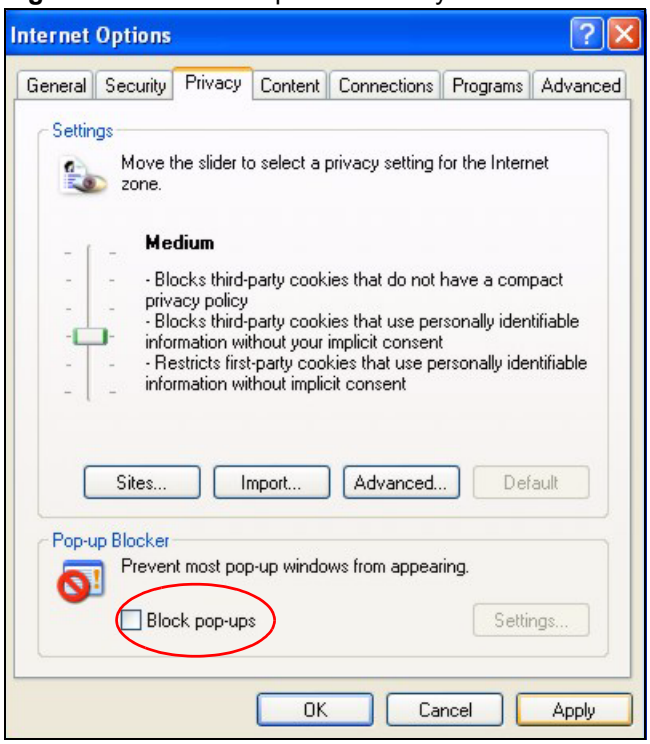


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 111 Internet Options: Privacy



3 Click **Apply** to save this setting.

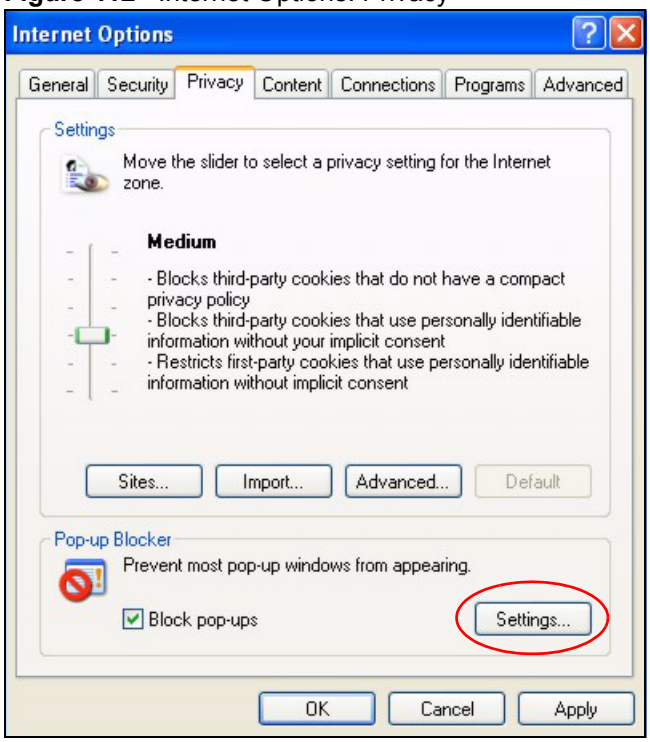
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

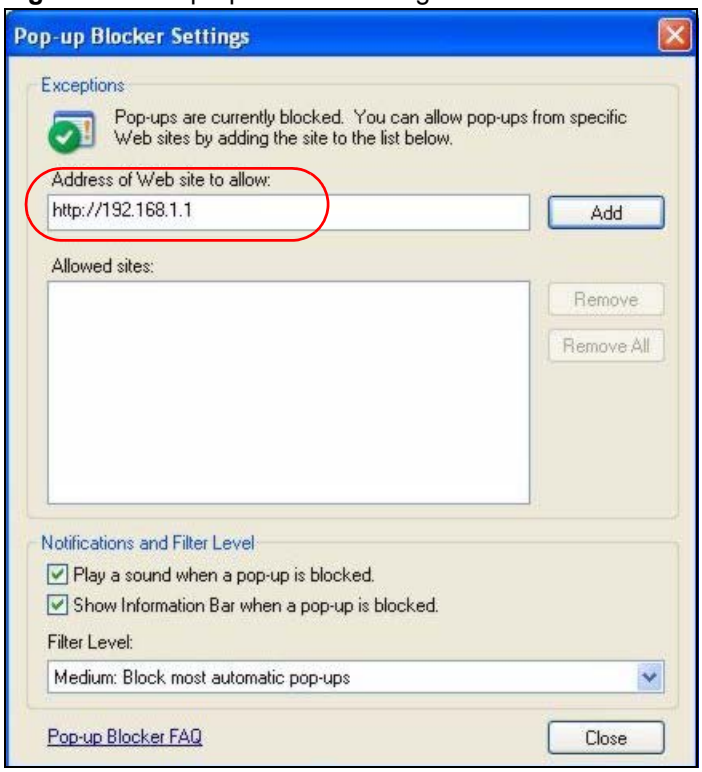
Figure 112 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 113 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

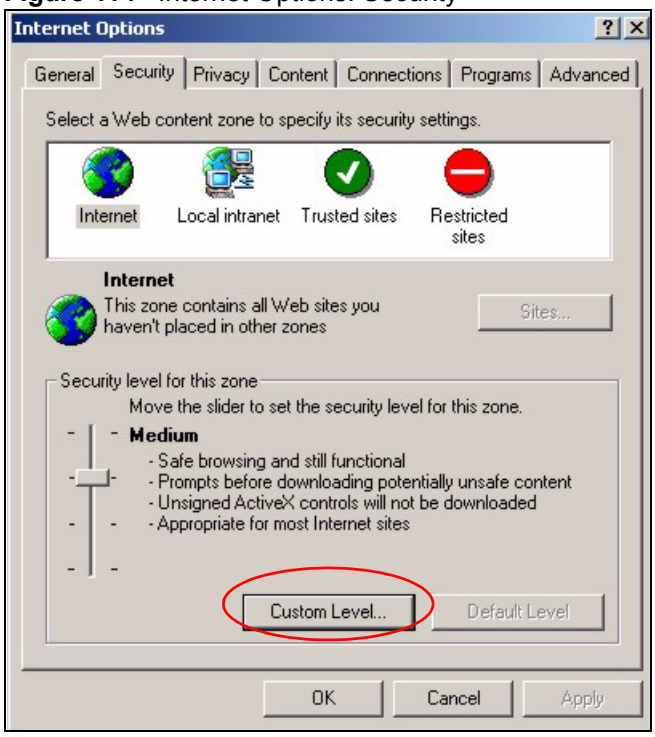
5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

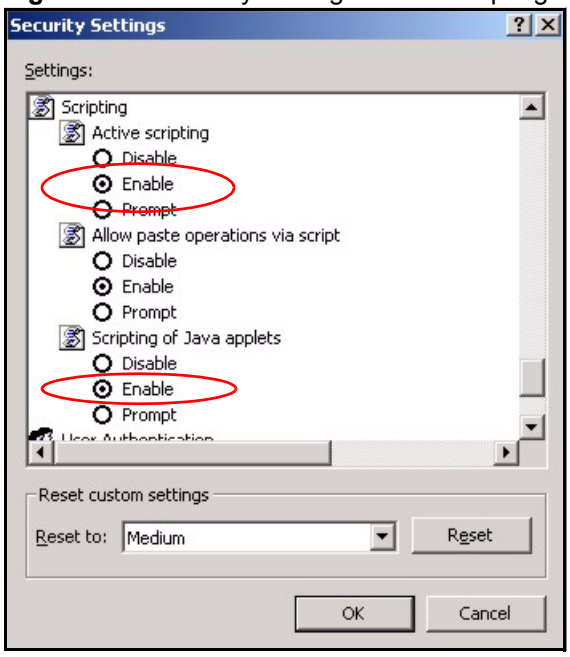
1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 114 Internet Options: Security



2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

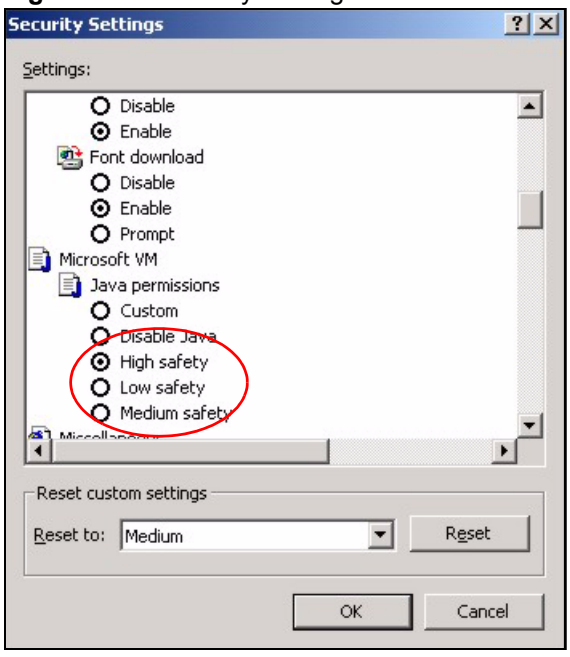
Figure 115 Security Settings - Java Scripting



Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

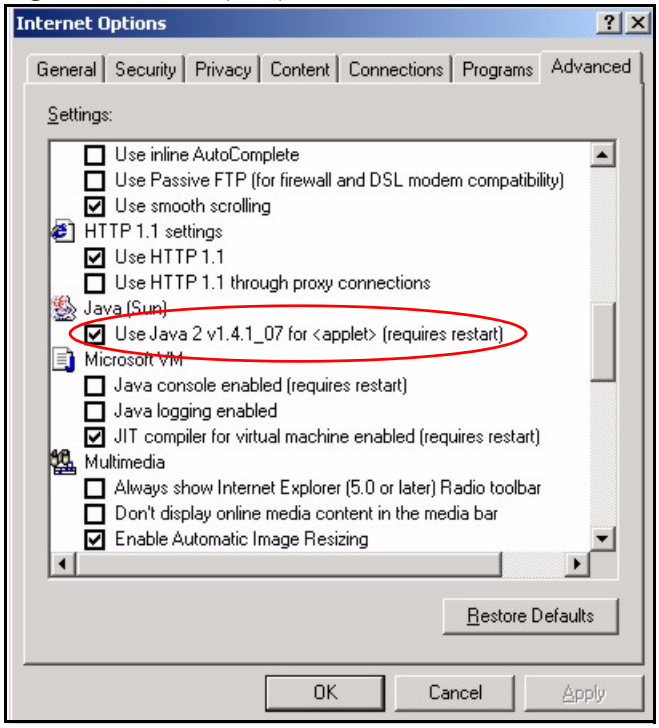
Figure 116 Security Settings - Java



JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3 Click **OK** to close the window.

Figure 117 Java (Sun)

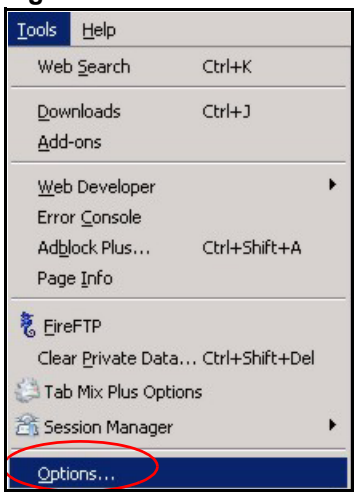


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

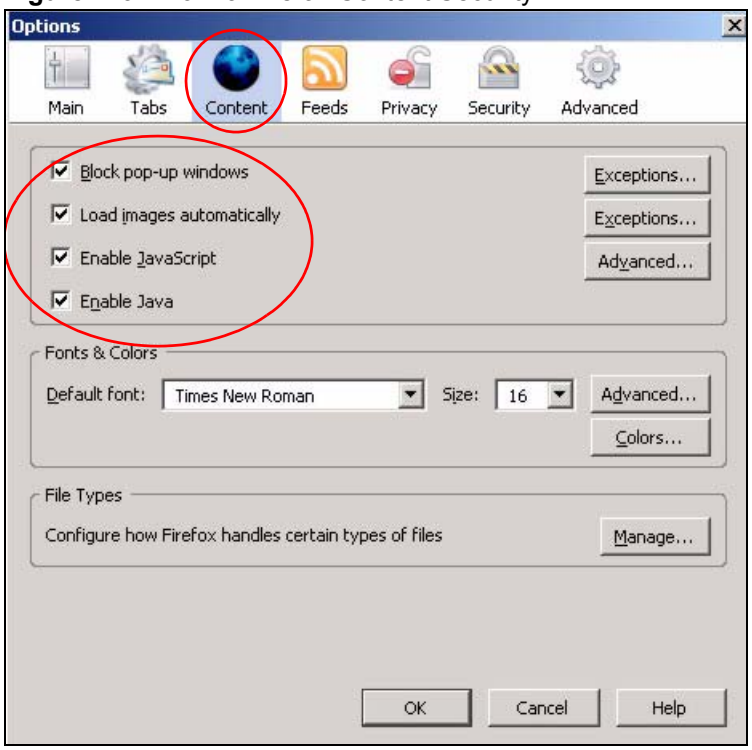
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 118 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 119 Mozilla Firefox Content Security



C

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

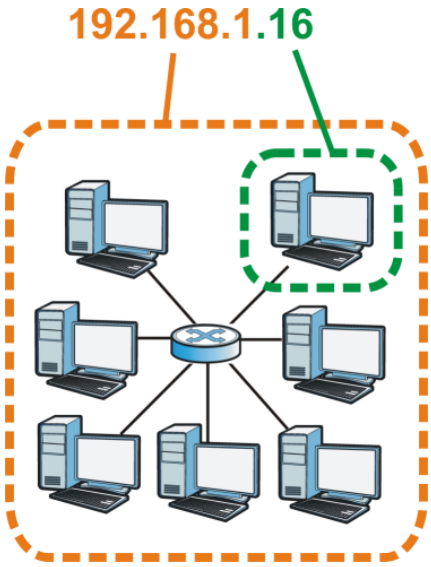
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 120 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 51 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 52 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 53 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 54 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 54 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

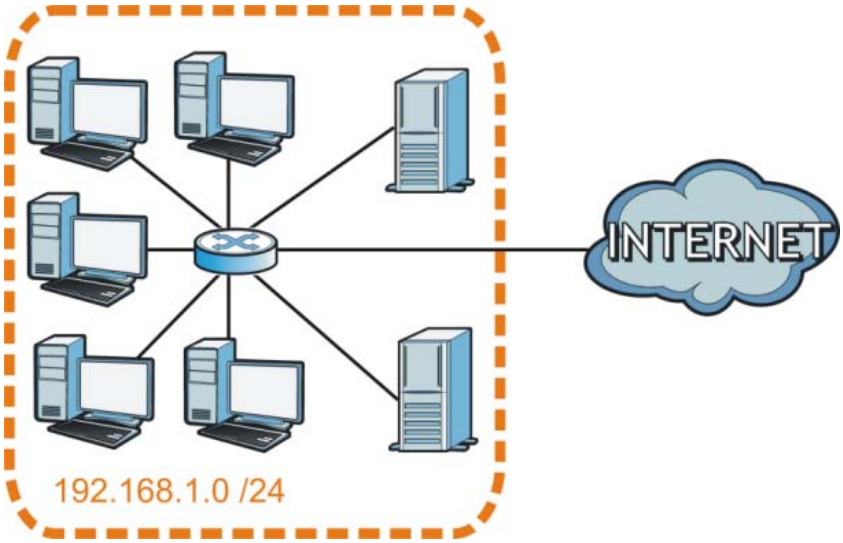
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 121 Subnetting Example: Before Subnetting

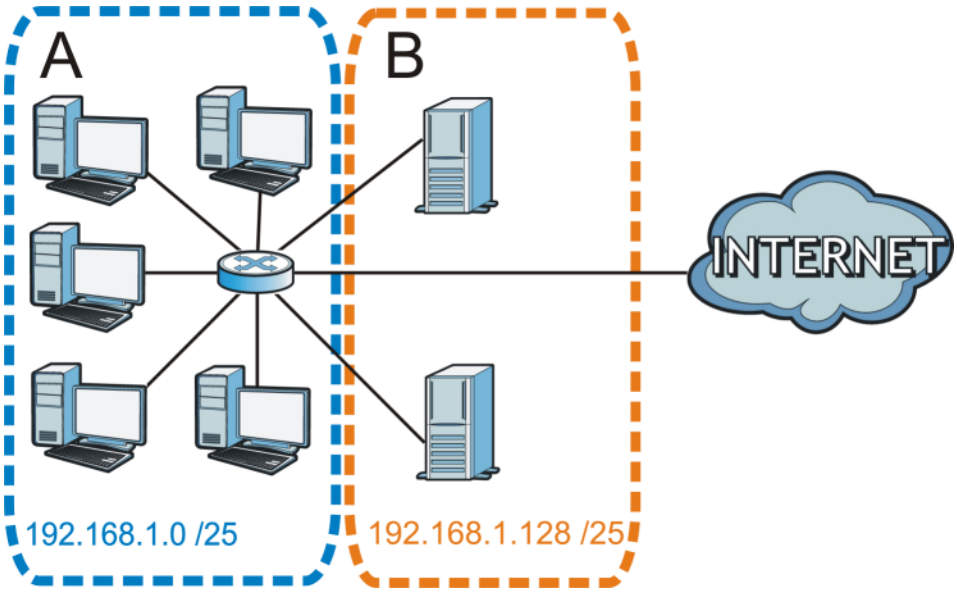


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 122 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 55 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 56 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 57 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 58 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 59 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 59 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 60 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 61 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 61 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

D

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 62 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.

Table 62 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.

Table 62 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 62 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

E

Legal Information

Copyright

Copyright © 2008 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the ZyXEL Device is subject to the terms and conditions of any related service providers.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

F

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

Numerics

802.1p 94, 96

A

access control 105
  activation 106
  configuration 106
  service type 106
activation
  access control 106
  CWMP 132
  DHCP 69
  DMZ 83
  dynamic DNS 130
  DYNDNS wildcard 130
  firewalls 102
  QoS 93
  SPI 102
  UPnP 118
address mapping 86
  types 87, 88
ADSL 99
  status 38
always-on connection 61, 65
application filter 112
ATM QoS 54, 56, 65, 66
  MBS 56
  PCR 56
  SCR 56

B

backup
  configuration 145, 146
broadcast 54

C

CBR 56, 66
CLI 27
Command Line Interface, see CLI
configuration
  access control 106
  backup 145, 146
  CWMP 132
  DHCP 69
  file 141
  firewalls 102
  IP precedence 94
  IP/MAC filter 111
  LAN 68
  port forwarding 85
  restoring 142
  SNMP 116
  static route 78
  WAN 55
connection
  always-on 65
CPE WAN Management Protocol, see CWMP
CWMP 131
  activation 132
  configuration 132

D

DDoS 101
DeMilitarized Zone, see DMZ
Denials of Service, see DoS
device information 37
  ADSL 38
  LAN 38
  WAN 38
DHCP 68, 69, 71
diagnostic 151
DiffServ Code Point, see DSCP
DMZ 83
  activation 83
DNS 68, 72
Domain Name System, see DNS
DoS 101
DSCP 94
dynamic DNS 129
  activation 130
  wildcard 129
    activation 130

Dynamic Host Configuration Protocol, see DHCP
DYNDNS wildcard 129
activation 130

E

encapsulation 53
PPPoA 60, 63
PPPoE 60, 63
RFC 1483 64

F

filters 109
application 112
IP/MAC 110
structure 109
IP/MAC filter
configuration 111
URL 109, 113
firewalls 101
configuration 102
DDoS 101
DoS 101
LAND attack 102
Ping of Death 102
SYN attack 101
firmware 141
upgrading 143
forwarding ports 82, 84
configuration 85
example 84
FTP 27
backing up configuration 145
limitations 142
restoring configuration 142, 143
upgrading firmware 143, 144

I

IGMP 54, 68, 74
Internet 53
ADSL 99
always-on connection 61, 65
ATM QoS 54, 56, 65, 66
encapsulation 53
IGMP 54
IP address 54, 58, 61, 64
MAC spoofing 57, 59, 61
MTU 57, 58, 61
multicast 54, 57, 59, 61
multiplexing 57, 58, 60, 62, 64
RIP 57, 59
RIPRouting Information Protocol, see RIP
setup 55
TCP MSS 61
VCI 55, 64
VPI 55, 64
Internet Group Multicast Protocol, see IGMP
IP address 54, 58, 61, 64, 67, 72
ping 151
private 73
IP precedence 94, 96
configuration 94
IP/MAC filter 110
configuration 111
structure 109

L

LAN 67
configuration 68
DHCP 68, 69, 71
DNS 68, 72
IGMP 68, 74
IP address 67, 72
multicast 68, 69, 74
RIP 68, 73
status 38
subnet mask 67, 72
LAND attack 102
LEDs 29
limitations
FTP 142
Local Area Network, see LAN
login 31
passwords 31, 137
logs 39

M

MAC spoofing 57, 59, 61
mapping address 86
types 87, 88
Maximum Burst Size, see MBS
Maximum Transmission Unit, see MTU
MBS 56, 65
metric 79
MTU 57, 58, 61

multicast 54, 57, 59, 61, 68, 69, 74
IGMP 54
multiplexing 57, 58, 60, 62, 64
LLC-based 64
VC-based 64

N

NAT 81, 82, 88, 89
address mapping 86
types 87, 88
DMZ 83
example 90
global 89
inside 89
local 89
outside 89
port forwarding 82, 84
configuration 85
example 84
status 82
SUA 82, 83
virtual server 84
example 84
Network Address Translation, see NAT
notation, subnet mask 199

P

passwords 31, 137
users 137
PCR 56, 65
Peak Cell Rate, see PCR
Permanent Virtual Circuit, see PVC
Ping of Death 102
port forwarding 82, 84
configuration 85
example 84
PPPoA 60, 63
PPPoE 60, 63
private IP address 73
PVC 54

Q

QoS 91
802.1p 94, 96
activation 93
DSCP 94
example 91
IP precedence 94, 96
priority queue 97
Quality of Service, see QoS

R

related documentation 3
remote management
SNMP 115
system timeout 106
reset 30
restart 149
restoring configuration 142
restrictions
FTP 142
RFC 1483 64
RIP 57, 59, 61, 68, 69, 73
Routing Information Protocol, see RIP

S

safety warnings 6
SCR 56, 65
Security Parameter Index, see SPI
setup
access control 106
DHCP 69
firewalls 102
IP precedenceQoS
IP precedence 94
IP/MAC filter 111
LAN 68
port forwarding 85
static route 78
WAN 55
Simple Network Management Protocol, see SNMP
Single User Account, see SUA
SNMP 27, 115
configuration 116
SPI 102
activation 102
static route 77
configuration 78
example 77
metric 79
status 33, 37
ADSL 38
LAN 38

NAT 82
traffic statistics 41
WAN 38
SUA 82, 83
subnet mask 67, 72, 198
notation 199
subnetting 200
Sustain Cell Rate, see SCR
SYN attack 101
syntax conventions 4
system
backing up configuration 145
backup configuration 145
firmware 141
upgrading 143
LED 29
login 31
logs 39
passwords 31, 137
users 137
reset 30
restoring configuration 142
status 33, 37
ADSL 38
LAN 38
WAN 38
time 139
traffic statistics 41

T

TCP Maximum Segment Size, see TCP MSS
TCP MSS 61
TFTP
upgrading firmware 144
time 139
TR-069 27
traffic statistics 41

U

UBR 56, 66
unicast 54
Universal Plug and Play, see UPnP
upgrading firmware 143
UPnP 117
activation 118
cautions 117
example 119
installation 119
NAT traversal 117
URL 109
URL filter 113
URL 109

V

VBR 66
VBR-nRT 56, 66
VBR-RT 56, 66
VCI 55, 64
Virtual Channel Identifier, see VCI
Virtual Path Identifier, see VPI
virtual server 84
example 84
VPI 55, 64

W

WAN 53
ADSL 99
always-on connection 61, 65
ATM QoS 54, 56, 65, 66
encapsulation 53
IGMP 54
IP address 54, 58, 61, 64
MAC spoofing 57, 59, 61
MTU 57, 58, 61
multicast 54, 57, 59, 61
multiplexing 57, 58, 60, 62, 64
RIP 57, 59, 61, 69
setup 55
status 38
TCP MSS 61
VCI 55, 64
VPI 55, 64
web configurator 27, 31
login 31
passwords 31
Wide Area Network, see WAN
wizard 45